Some Remarks on Lengths of Propositional Proofs

Samuel R. Buss*

Department of Mathematics
University of California, San Diego

July 3, 2002

Abstract

We survey the best known lower bounds on symbols and lines in Frege and extended Frege proofs.

We prove that in minimum length sequent calculus proofs, no formula is generated twice or used twice on any single branch of the proof.

We prove that the number of distinct subformulas in a minimum length Frege proof is linearly bounded by the number of lines. Depth d Frege proofs of m lines can be transformed into depth d proofs of $O(m^{d+1})$ symbols.

We show that renaming Frege proof systems are p-equivalent to extended Frege systems.

Some open problems in propositional proof length and in logical flow graphs are discussed.

1 Preliminaries

This paper considers the lengths of proofs of propositional tautologies; we measure proof length either by counting the number of lines (formulas) in the proof or by counting the number of symbols in the proof.

*Supported in part by NSF grant DMS-9205181

The first three sections give lower bounds on proof lengths which are quite easy to obtain and yet represent the best currently-known lower bounds. The contents of sections 1-3 have already appeared in prior work, but they are fundamental and are not widely known, so we feel it is useful to exposite them here. This author first discovered the results of sections 2 and 3 from considering the logical-flow graph [4]; however, the proofs presented in this paper are much simpler. Other prior work with results similar to the contents of sections 2 and 3 includes Cejtin-Čubarjan[7], Buss-et al. [6], Krajíček [11, 10], Bonet [1], Bonet-Buss [2], and Buss [5].

In section 4, we define a new version PK of the propositional sequent calculus and pose the problem of finding a $(1+\epsilon)n$ lower bound on the size of PK-proofs. We give the currently best known lower bound of $n+\Omega(n^{1/3})$.

In section 5, it is shown that in minimum length tree-like PK-proofs, no formula is introduced twice as a conclusion or used twice as a hypothesis on any single branch in the proof.

In section 6, we discuss the open problem of whether cycles can eliminated from the logical flow graph of a proof without a superpolynomial size penalty.

In section 7, we prove a new result showing the equivalence of constant-depth Frege proofs with polynomially many lines and constant-depth Frege proofs with polynomially many symbols.

In section 8, we prove that the variable renaming inference rule is unexpectedly powerful, in that renaming Frege proof systems are p-equivalent to extended Frege proof systems.

We work first with Frege systems, which are generalizations of the usual textbook proof systems for propositional logic based on modus ponens. We also work with two extensions of Frege systems, namely, extended Frege systems and substitution Frege systems. This section briefly reviews the definitions of these systems.

A *proof* consists of a directed acyclic graph with each node labeled by a propositional formula; there is one node with outdegree zero, which is labeled with the formula that is proved. Each formula in the proof is derived from its immediate predecessors by one of a finite set of schematically defined rules of inference. A schematically defined rule of inference is defined by a figure of the form:

$$\frac{A_1 \quad \cdots \quad A_k}{B}$$

where the formulas $A_1, \ldots, A_k$ and B contain propositional variables $p_1, \ldots, p_m$. A substitution σ consists a mapping from propositional variables to propositional formulas. If A is a formula, then $A\sigma$ denotes the result of applying the substitution to A, which replaces each variable p_i in A with its image under σ. The above rule of inference allows $B\sigma$ to inferred from the hypotheses $A_1\sigma, \ldots, A_k\sigma$, for σ any substitution.

As two examples of rules of inference consider:

$$\frac{}{p_1 \rightarrow (p_2 \rightarrow p_1)} \qquad \text{and} \qquad \frac{p_1 \qquad p_1 \rightarrow p_2}{p_2}.$$

The left figure shows an inference with zero hypotheses (i.e., an axiom) and indicates that any substitution instance of the formula $p_1 \rightarrow (p_2 \rightarrow p_1)$ is a valid axiom. The right figure is the usual inference of modus ponens.

The definition of a *Frege proof system* is as follows: it uses a finite, complete set of propositional connectives and it has a finite set of schematically defined rules of inference; furthermore, it must be sound and complete, i.e., it must admit modus ponens as a derived rule of inference and it must prove every tautology.

The most commonly used Frege systems have a finite set of axiom schemes and have modus ponens as the only additional rule of inference. However, clearly many other choices of rules of inference are possible. The most common choices for the propositional connectives include $\neg$, $\land$, $\lor$, $\rightarrow$; but any complete set of connectives is permissable. Of course, the choice of propositional connectives and rules of inference will affect the lengths of proofs; however, it is known that these choices only change the lengths of proofs by polynomial amounts. The most general result of this type is that any Frege system $\mathcal{F}_1$ can p-simulate any other Frege system $\mathcal{F}_2$, which means that if a tautology A has an $\mathcal{F}_2$-proof P of m symbols, then there is a natural translation A' of A into the language of $\mathcal{F}_1$ such that A' has an $\mathcal{F}_1$-proof P' of length $\leq p(m)$ symbols, where p is a polynomial, and further A' and P' may be obtained by a polynomial time algorithm from P (see [15, 8] for a detailed development of this). The polynomial p and the polynomial algorithm depend only the proof systems $\mathcal{F}_1$ and $\mathcal{F}_2$.

If the Frege systems $\mathcal{F}_1$ and $\mathcal{F}_2$ have the same language, then we have a much better simulation: there must exist a constant c such that any $\mathcal{F}_2$-proof of m lines and n symbols can be transformed into an $\mathcal{F}_1$-proof of $\leq cm$ lines and $\leq cn$-symbols. This is easy to prove from the fact that the rules of inference of $\mathcal{F}_2$ must be derived rules of inference for $\mathcal{F}_1$ and from the fact that the rules of inference are schemes.

Two commonly studied extensions of Frege systems are the extended Frege systems and the substitution Frege systems. A *substitution Frege system* consists of a Frege system augmented with the substitution rule with inferences of the form

$$\frac{A}{A\sigma}$$

for any substitution σ. In other words, any instance of A can be inferred from A.[†]

An *extended Frege system* consists of a Frege system augmented with the extension rule. The extension rule allows the inference of a formula:

$$p \leftrightarrow A$$

where A is any formula and p is a variable which does not occur in A, does not appear in any earlier extension rule, and does not occur in the final formula in the proof (the formula being proved). The variable p is called the *extension variable*. The idea of the extension rule is to allow the variable p to act as an abbreviation for the formula A; the purpose of using abbreviations is to (potentially) reduce the number of symbols in proofs.

It is known that any two extended Frege proof systems p-simuluate each other and that any two substitution Frege systems p-simulate each other; furthermore, a substitution Frege system p-simulates an extended Frege proof system [8, 15]. Also, an extended Frege proof system p-simulates a substitution Frege proof system [9, 12]

[†]Our definition of substitution Frege system allows the simultaneous substitution of multiple formulas for multiple variables of A. Other authors have allowed substitution for only one variable at a time. It is easy to see that single variable substitition can polynomially simulate simultaneous substitution. However, it is possible that our simultaneous substitution provides some speedup over the single variable substitution rule.

We prove in section 8 that the substitution rule restricted to variable renamings is as powerful as the full substitution rule.

More information on Frege systems and proof lengths can be found in the original works of Cook-Reckhow [8], Reckhow [15] and Statman [16].

The author thanks M. L. Bonet, J. Krajíček and T. Pitassi for helpful discussions as this paper was being written.

2 Active Subformulas

In this section we introduce the notion of *active* subformulas in a proof. This will allow us to bound the number of distinct subformulas occuring in a Frege or extended Frege proof.

We shall henceforth assume that we have a fixed Frege proof system in mind, with a fixed, finite set of connectives and rules of inference. For convenience sake, we shall assume that the 0-ary connectives $\top$ and $\bot$ are included in the propositional language; these are the constants *True* and *False*. This assumption is not essential for our results, but will simplify some of our examples.

Recall that if A is a formula and σ is a substitution, then $A\sigma$ is a formula. Consider a subformula C of $A\sigma$. Obviously, the principal connective of C either corresponds to a connective in A or was introduced by the application of σ to A.

Now let σ be a substitution and consider an inference schematically defined as in section 1 above. Consider the inference I

$$\frac{A_1\sigma \quad \cdots \quad A_k\sigma}{B\sigma}$$

which is the instance of the rule of inference induced by σ. Let C be an occurence of a subformula in any one of $A_1\sigma, \ldots, A_k\sigma, B\sigma$. We define C to be *active with respect to the inference I* if and only if the principal connective of C was not introduced by σ (and thus the principal connective of C corresponds to a connective that already appears in the schematic definition of the rule of inference).

If P is a Frege proof, and C is an occurence of a subformula in a formula in P, we say that C is *active in the proof P* if and only if there is at least one inference in P such that C is active w.r.t. that inference. Finally if C is a formula, we say that C is *active somewhere in* P iff there is at least one occurence of C as a subformula in P which is active in P. If is not the case the C is active somewhere in P, then we say that C is *not active anywhere in* P.

Lemma 1 *Let P be a $\mathcal{F}$-proof and C be a formula which is not active anywhere in P. Let D be an arbitrary formula. Let $P(D/C)$ be obtained by replacing every occurence of C as a subformula in P with D. Then $P(D/C)$ is a valid $\mathcal{F}$-proof.*

Proof It will suffice to show that if no occurence C is active w.r.t. a given inference I in P, then replacement of C by D preserves the validity of the inference I. The inference I is formed by the application of some substitution to a schematic rule of inference. Since C is not active, it must be that every occurence of C in the inference I was introduced wholly by the substitution; hence, uniformly replacing C with D yields another valid inference. □

We can extend the notion of "active subformula" to extended Frege proofs. For inferences given by schematic rules there is no change to the notion of active. For an extension rule inference of the form $p \leftrightarrow A$, the formulas p and $p \leftrightarrow A$ are defined to be the only subformulas which are active with respect to this inference. The above lemma holds also for extended Frege proofs, modulo avoiding conflicts with extension variables:

Lemma 2 *Let P be an $e\mathcal{F}$-proof and C be a formula which is not active anywhere in P. Let D be an arbitrary formula such that no extension variable of P occurs in D. Let $P(D/C)$ be obtained by replacing every occurence of C as a subformula in P with D. Then $P(D/C)$ is a valid $e\mathcal{F}$-proof.*

The proof of Lemma 2 is exactly like the previous proof, except that it must now be noted that extension inferences remain valid since no new occurences of extension variables are introduced.

Let $||A||$ denote the number of *distinct* subformulas of A. We can now use the notion of active subformulas to bound the number of distinct subformulas occuring in a proof:

Theorem 3 *Let P be a $\mathcal{F}$-proof or an $e\mathcal{F}$-proof of a formula A containing m lines. Then there is a $\mathcal{F}$-proof or an $e\mathcal{F}$-proof (respectively) of A in which only $O(m) + ||A||$ many distinct subformulas occur.*

Proof If P contains any subformulas which are not active anywhere in P and which do not occur as a subformula of A, then replace them with an arbitrary variable (or with $\top$ or $\bot$ if preferred). By the above lemma, this yields a valid proof of A. So we can assume w.l.o.g. that every subformula occuring in P either is equal to a subformula of A or is active somewhere in P. But since there are only a finite set of schematic rules of inference, there is a maximum number c of subformula occurences which can be active with respect to any single inference. Thus there are at most $cm + ||A||$ many distinct subformulas occuring in P. $\Box$

Theorem 4 *Suppose that A has an m line Frege or extended Frege proof P. Then there is a formula B such that $||B|| = O(m)$ and such that B also has an m-line Frege or extended Frege proof and such that A is a substitution instance of B.*

Proof Replace, one at a time, the subformulas of A which are not active anywhere in P by new distinct variables. The result is a proof of m lines of a formula B, of which A is a substitution instance. $\Box$

3 Lower Bounds on Proof Lengths

In this section, we survey some lower bounds on the number of symbols and lines in Frege and extended Frege proofs. The lower bounds we obtain here are the best bounds presently known for any propositional formulas.

The first lower bound is a lower bound on the number of lines in a Frege or extended Frege proof. It is an immediate corollary of Theorem 4 above.

Theorem 5 *If A is a tautology which is not a substitution instance of a shorter tautology, then any Frege or extended Frege proof of A requires $c \cdot ||A||$ lines, where c is a constant symbol depending only on the proof system.*

Our lower bound on the number of symbols in a Frege or extended Frege proof of A will be expressed in terms of the total size of the subformulas of A. We define the *size* of a formula to equal the number of symbols in the formula, and we define $||A||_\Sigma$ to be equal to the sum of the sizes of all *distinct* subformulas of A. Note that this means that if a subformula occurs twice in A, we still count its size only once.

Theorem 6 *Suppose A is a tautology which is not a substitution instance of a shorter tautology. Then any Frege or extended Frege proof of A contains at least $c \cdot ||A||_\Sigma$ symbols, where c is a constant depending only on the proof system.*

Proof Let P be a Frege or extended Frege proof of P. Since A is not a substitution instance of a shorter tautology, then every non-atomic subformula of A must be active somewhere in the proof. This is because otherwise, any non-atomic subformula of A which is not active anywhere could be globally replaced by a new variable, yielding a proof of a shorter tautology.

Consider a given symbol in the proof P: this symbol may occur in zero, one or more active subformula occurences. For example, suppose a Frege proof contains the lines B, $B \to (C \to B)$ and $C \to B$ where the second line is introduced by an axiom and the third by modus ponens. The formula $B \to (C \to B)$ is active both w.r.t. the axiom inference and w.r.t. the modus inference. Its subformula $C \to B$ is active w.r.t. the axiom inference (since the axiom scheme $p_1 \to (p_2 \to p_1)$ explicitly contains its principal connective). Thus, if α is any symbol occurence inside the occurence of C as a subformula of the second formula or inside the second occurence of B in the second formula, then we have α occuring inside exactly two different active subformula occurences.

Now we claim that there is a constant d such that every symbol in P is in at most d different active subformula occurences in P. This is because the inference rules of the proof system are given schematically, and thus, there is a maximum depth d so that any active subformula occurence has its root (principal connective) occuring at depth $< d$ in a formula occuring in the proof. From this it follows that the number of symbols in the proof P is at least $\frac{1}{d}||A||_\Sigma$. $\Box$

As an application of our two lower bounds on proof length, consider the formula $\top^k$, defined as

$$\bot \vee (\bot \vee (\bot \vee \cdots (\bot \vee \top) \cdots)),$$

where there are k $\bot$'s. Clearly this a tautology, but is not an instance of a shorter tautology. Thus by Theorem 5, any Frege or extended Frege proof of $\top^k$ requires $\Omega(k)$ lines and $\Omega(k^2)$ symbols. Since $\top^k$ has $O(k)$ symbols, these are *linear* lower bounds on the number of lines and *quadratic* lower bounds on the number of symbols.

Somewhat surprisingly, these are the best lower bounds known for Frege and extended Frege proof systems. That is to say, that all currently known lower bounds for Frege or extended Frege proofs, are contained in Theorems 5 and 6. Indeed, it is consistent with our current state of knowledge that every tautology has a Frege proof containing a linear number of lines and a quadratic number of symbols. The best known upper bounds on the size of Frege proofs are exponential, and it is commonly conjectured that some tautologies do require (near) exponential size proofs. Thus there is a large gap between the upper and lower bounds.

A attractive, but dificult, open problem is to is to give even a small improvement on the bounds of Theorems 5 and 6. Some work in this direction has been done in the work of Bonet [1]: she considers two families of tautologies consisting balanced formulas (i.e., have depth $O(\log n)$) which were chosen in the hopes that they would require long Frege proofs; nonetheless, she obtained Frege proofs of these formulas of symbol sizes $O(n \log^2(n))$ and $O(n \log^3 n)$. Theorem 6 gives lower bounds of $O(n \log n)$ on the symbol size of their Frege proofs; hence there is only a (poly)logarithmic factor between the upper and lower bounds. The problem of showing Bonet's upper bounds to be optimal seems quite difficult.

Another example of balanced tautologies that may require Frege proofs of more than $O(n \log n)$ symbols is the propositional pigeonhole priniciple (PHP). The polynomial size Frege proofs of PHP given in Buss [3] are significantly larger than $n \log n$ (here n is to be the number of symbols in the PHP formula, so n is cubic in the number of 'holes' and 'pigeons', see [3] for the formulation of PHP). But it seems very difficult to prove that

PHP does not have Frege proofs of $O(n \log n)$ symbols.

Finally, we can use Theorems 5 and 6 to separate extended Frege proof lengths from substitution Frege proof lengths. This done by noting that the formulas $\top^k$ have substitution Frege proofs of $O(\log n)$ lines and $O(n)$ symbols. These substitution Frege proofs proceed as follows (assume for simplicity that k is a power of two, but the same ideas work for general k): Let p^k denote the formula $\perp \vee (\perp \vee \cdots (\perp \vee p) \cdots)$ containing k $\perp$'s. First derive

$$p \to p^1 \qquad \text{i.e., } p \to (\perp \vee p)$$

with a constant size proof. Then assuming that $p \to p^m$ has already been derived, use the substitution rule to substitute p^m for p to obtain $p^m \to p^{2m}$. From these two formulas, use a finite number of steps to derive $p \to p^{2m}$. After $\log k$ iterations, one obtains $p \to p^k$. Clearly this proof has $O(\log k)$ lines and $O(k)$ symbols. Thus we have proved:

Theorem 7 *(See [11] and [7]) There are tautologies which have substitution Frege proofs of $O(h)$ lines and $O(k)$ symbols but which require extended Frege proofs of $\Omega(2^h)$ lines and $\Omega(k^2)$ symbols.*

It is well-known that substitution Frege and extended Frege proof systems can p-simulate each other. The best simulations (measuring proof length by number of lines) that we have been able to obtain are: (1) substitution Frege proofs can quadratically simulate extended Frege proof systems (the 'standard' simulation of [8] is cubic, but it can be improved to quadratic using Bonet's theorem that Frege systems can quadratically simulate the 'simple' deduction theorem [1]); and (2) extended Frege proofs can cubicly simulate substitution Frege proofs (Dowd's original proof gave no information on the polynomial degree, but a cubic simulation can be obtained by a very minor modification of the proof of Krajíček-Pudlák [12]).

It would be interesting to obtain superlogarithmic lower bounds on the number of lines in subsitution Frege proofs or superlinear lower bounds on the number of symbols in substitution Frege proofs. For this, recall that we are allowing simultaneous substitution.

4 A sequent calculus system

We next introduce a variant of the sequent calculus for propositional logic. We use sequent calculus rules which are slightly different from the usual sequent calculus formulations but have the advantage of being better suited to precisely proof length measurements. We presume the reader has some familiarity with the sequent calculus as contained in the first sections of [17].

Definition The sequent calculus PK allows as initial sequents any sequent $A \to A$. The rules of inference of PK are:

Weak Structural Rules

Exchange:left $\dfrac{\Gamma, A, B, \Pi \longrightarrow \Delta}{\Gamma, B, A, \Pi \longrightarrow \Delta}$ *Exchange:right* $\dfrac{\Gamma \longrightarrow \Delta, A, B, \Lambda}{\Gamma \longrightarrow \Delta, B, A, \Lambda}$

Contraction:left $\dfrac{A, A, \Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta}$ *Contraction:right* $\dfrac{\Gamma \longrightarrow \Delta, A, A}{\Gamma \longrightarrow \Delta, A}$

Weakening:left $\dfrac{\Gamma \longrightarrow \Delta}{A, \Gamma \longrightarrow \Delta}$ *Weakening:right* $\dfrac{\Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, A}$

The weak structural rules are also referred to as just *weak* inference rules. The rest of the rules are called *strong* inference rules.

The Cut Rule

$$\frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

The Propositional Rules

$$\neg\text{:}\textit{left}\ \frac{\Gamma \longrightarrow \Delta, A}{\neg A, \Gamma \longrightarrow \Delta} \qquad \neg\text{:}\textit{right}\ \frac{A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta, \neg A}$$

$$\wedge\text{:}\textit{left}\ \frac{A, B, \Gamma \longrightarrow \Delta}{A \wedge B, \Gamma \longrightarrow \Delta} \qquad \wedge\text{:}\textit{right}\ \frac{\Gamma \longrightarrow \Delta, A \qquad \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \wedge B}$$

$$\vee\text{:}\textit{left}\ \frac{A, \Gamma \longrightarrow \Delta \qquad B, \Gamma \longrightarrow \Delta}{A \vee B, \Gamma \longrightarrow \Delta} \qquad \vee\text{:}\textit{right}\ \frac{\Gamma \longrightarrow \Delta, A, B}{\Gamma \longrightarrow \Delta, A \vee B}$$

$$\rightarrow\text{:}\textit{left}\ \frac{\Gamma \longrightarrow \Delta, A \qquad B, \Gamma \longrightarrow \Delta}{A \rightarrow B, \Gamma \longrightarrow \Delta} \qquad \rightarrow\text{:}\textit{right}\ \frac{A, \Gamma \longrightarrow \Delta, B}{\Gamma \longrightarrow \Delta, A \rightarrow B}$$

Note that we have stated the $\wedge$*:left* and $\vee$*:right* differently than usual; we feel that our definitions give a better definition of proof length (without changing proof lengths by more than a constant factor).

Definition PK-proofs are directed acyclic graphs of sequents, in which each node is inferred from its predecessors by a valid rule of inference. The *strong inference length* of a PK proof P is denoted $||P||_{dag}$ and is equal to the number of strong inferences in P. When we restrict attention to tree-like proofs P, then the strong inference length of P is denoted $||P||$.

Definition A formula occuring in an inference is *active* if and only if the inference is a propositional inference and the formula is the principal formula of the inference.

It is obvious that Lemmas 1 and 2 hold also for the sequent calculus PK. Also, Theorems 3, 4 and 5 will hold for PK in place of $\mathcal{F}$ and $e\mathcal{F}$, even if m is the strong inference length instead of the line length. Theorem 5 can be sharpened for PK to give:

Theorem 8 *Let $\Gamma \longrightarrow \Delta$ be a valid sequent which is not a substitution instance of a smaller valid sequent. Let m equal the number of distinct non-atomic formulas in $\Gamma \longrightarrow \Delta$. Then any PK-proof of $\Gamma \longrightarrow \Delta$ requires at least m strong inferences.*

The idea of the proof of Theorem 8 is exactly like the idea behind Theorem 5; that is, every subformula of $\Gamma \longrightarrow \Delta$ must be the principal formula of a strong inference in any proof of $\Gamma \longrightarrow \Delta$. We leave it to the reader to check the details of this proof.

One of our main reasons for introducing PK is to state the following challenge problem:

Problem: Find a family of valid sequents whose PK-proofs require more than $(1+\epsilon)\cdot m$ strong inferences with ϵ a constant strictly greater than zero (where m measures the number of distinct non-atomic subformulas in the sequents).

The best partial solutions to this challenge problem that we have been able to obtain is that any PK-proof of the tautologies that express the pigeonhole principle require at least $m + (1-\epsilon)(m^{1/3})$ strong inferences, for any $\epsilon > 0$ and m sufficiently large. To prove this, let P be a *shortest* PK-proof of the sequents PHP_n^{n+1} expressing the $n+1$ into n pigeonhole principle. The number of distinct non-atomic subformulas in the sequent PHP_n^{n+1} is $m = n^3 + o(n^3)$. Let p equal the number of distinct non-atomic subformulas which appear in P but not in its endsequent PHP_n^{n+1}. By considerations similar to Theorem 8, P has at least $m+p$ strong inferences.[‡] If $p > (1-\epsilon)n$, then we are done. Otherwise, it is not difficult to see that it is possible to find a partial truth assignment which sets $< p$ many values of $f(i)$ such that all the formulas which appear in P but not PHP_n^{n+1} have depth one (i.e. contain only one logical connective). Note that setting $f(i) = j$ means choosing a restriction in which p_{ij} is set to the constant *True* and $p_{i,j'}$ and $p_{i',j}$ are set to *False* for all $i \neq i'$ and $j \neq j'$: once the restriction is chosen then the formulas are collapsed to remove the constants *True* and *False* and then any inferences which have been trivialized by this process are removed from the proof. After this restriction, at least $\delta \cdot n$ elements remain in the domain and range of f (where $\delta > 0$ is a constant depending on ϵ) and we are left with a constant depth propositional proof of the pigeonhole principle $PHP_{\delta n}^{\delta n+1}$: this constant depth proof must be exponential size by [13, 14].

[‡]Note that, without loss of generality, every subformula appearing in the proof P must be the same formula as the principal formula of some inference in P, since otherwise, the number of distinct subformulas in P could be reduced by the methods used to prove Theorem 8.

5 Non-repetition of formulas

We now prove a normal form theorem for PK-proofs which states that in a shortest tree-like PK-proof, there is no formula which occurs twice on a one branch in the proof as an auxiliary formula in the antecedent (or in the succedent) of a strong inference or twice on a branch as a principal formula of a strong inference.

In this section, we will always assume that P denotes a tree-like PK-proof of minimum strong inference length; this means that there is no P' with the same endsequent as P such that $||P'|| < ||P||$.

Definition A *branch* in P is a path through the proof P viewed as a directed acyclic graph starting with an initial sequent and ending with the endsequent.

Definition An occurrence of a formula in P is called a *strong auxiliary* formula if it is an auxiliary formula of a strong inference. Likewise, a *strong principal* formula is an occurrence of a formula as the principal formula of a strong inference.

A *succedent* formula (respectively, *antecedent* formula) is an occurrence of a formula in a succedent (respectively, antecedent).

Theorem 9 *Let P be a tree-like PK-proof of minimum strong inference length and π be a branch of P. Then there is no formula A which occurs twice as a strong auxiliary antecedent formula on the branch π. Likewise, there is no formula A which occurs twice as a strong auxiliary succedent formula on the branch π.*

A corollary of Theorem 9 is that no formula is used twice as a cut formula on any branch in a proof P of minimum strong inference length.

Proof Suppose, for sake a contradiction, that the branch π contains two uses of A as a strong auxiliary succedent formula. Let I_1 and I_2 be the two strong inferences which involve the two uses of A as a strong auxiliary succedent formula. Let S_1 be the lower sequent of I_1, and S_2 be the upper sequent of I_2. Let B be the principal formula of I_1. Thus, S_1 is a sequent of the form

$$S_1 \;=\; \Gamma \longrightarrow \Delta, B \qquad \text{or} \qquad S_1 \;=\; B, \Gamma \longrightarrow \Delta$$

where B may be missing if I_1 is a cut infererence.

Now modify the proof P as follows: First, for every sequent $\Pi \longrightarrow \Lambda$ which lies on π between S_1 and S_2, inclusively; replace $\Pi \longrightarrow \Lambda$ with $\Pi^- \longrightarrow A, \Lambda^-$, where Π^- and Λ^- are obtained by removing the descendent (if any) of B from Π or Λ. Second, every sequent $\Pi \longrightarrow \Lambda$ on π below S_2, is replaced with $\Pi^- \longrightarrow \Lambda^-$. This, of course, will cause P to be no longer be a valid proof; however, it is easy to further modify P to be a valid proof by adding only weak inferences. This includes replacing the strong inference I_1 with weak inferences and, if I_1 has two upper sequents, removing one them from the proof. Also, some other strong inferences between I_1 and I_2 may need to be replaced in the same way with weak inferences. In addition, the upper sequent of I_2 will now contain two occurrences of A, these are contracted with weak inferences before being used as a hypothesis to I_2; and therefore, it is permissable for A to not appear in the lower sequent of I_2. Finally, some new weakening inferences may be needed at the end of the proof. We have thus constructed a valid proof with fewer strong inferences than P, which contradicts the choice of P.

The case where the strong auxiliary formula A occurs in the antecedent is similar. □

Theorem 9 also holds for the usual formulation of the sequent calculus (recall that the usual formulation has different $\lor$*:right* and $\land$*:left* inferences). The same proof still works without modification.

Theorem 10 *Let P be a tree-like PK-proof of minimum strong inference length. Then there is no formula A which occurs twice as a strong principal antecedent formula on a branch π. Likewise, there is no formula A which occurs twice as a strong principal succedent formula on a branch π.*

Proof This is an immediate consequence of Corollary 9 because of the definition of the the rules of inference of PK. To see this, suppose that a branch π contains two strong inferences I_1 and I_2 with the same principal formula A. By examination of the rules of PK, I_1 and I_2 have the same auxiliary formulas. Now taking a branch π' containing I_1, I_2 and (one of) the upper sequents of the upper strong inference, we have the same formula used twice on π' as a strong auxiliary formula so as to violate the condition of Theorem 9. $\Box$

Theorem 10 apparently does not hold for the usual formulation of the sequent calculus, which has different $\lor$*:right* and $\land$*:left* inference rules than PK. For example, with the usual $\lor$*:right* rules, a proof could contain

$$\dfrac{\Gamma \longrightarrow \Delta, A}{\Gamma \longrightarrow \Delta, A \lor B}$$

$$\vdots$$

$$\dfrac{\dfrac{\Pi \longrightarrow \Lambda, A \lor B, B}{\Pi \longrightarrow \Lambda, A \lor B, A \lor B}}{\Pi \longrightarrow \Lambda, A \lor B}$$

Theorem 11 *In a tree-like PK-proof of minimum strong inference length, there is no branch π on which a formula has an occurrence as a strong auxiliary antecedent formula above an occurence as a strong principal antecedent formula.*

The same holds for "succedent" replacing "antecedent".

The proof of Theorem 11 is essentially identical to the proof of Theorem 9. We omit the proof and leave it to the reader to supply one. (The primary difference is to now take S_2 to be the *lower* sequent of I_2.)

Theorem 11 also holds for the usual formulation of the propositional sequent calculus in place of PK.

Theorem 12 *In a tree-like PK-proof of minimum strong inference length, no formula appears twice as a strong principal formula on a single branch.*

Note that the difference between Theorem 10 and Theorem 12 is that we are no longer considering strong principal formulas which both occur in the antecedent or both occur in the succedent.

Proof Suppose, for a contradiction, that P is a PK-proof of minimum strong inference length with a branch π that contains two strong inferences I_1 and I_2 which have the same principal formula A. Let I_1 be above I_2.

Without loss of generality, assume that I_1's principal formula occurs in the antecedent and hence, by Theorem 10, I_2's principal formula occurs in the succedent. Let I_1 and I_2 have lower sequents S_1 and S_2 of the forms

$$S_1 \;=\; A, \Gamma_1 \longrightarrow \Delta_1 \qquad \text{and} \qquad S_2 \;=\; \Gamma_2 \longrightarrow \Delta_2, A.$$

Modify the proof P as follows. First, replace the sequent S_1 with the sequent $S_1' \;=\; A, \Gamma_1 \longrightarrow A, \Delta_1$. Note that S_1' can be proved with zero strong inferences; thus, we also replace the entire subproof of P ending at the strong inference I_1, with a new subproof of S_1' which has no strong inferences. Second, replace each sequent $\Pi \longrightarrow \Lambda$ below S_1 and above S_2 with the sequent $\Pi \longrightarrow A, \Lambda$. Finally, the sequent S_2 is replaced by the weak inferences

$$\frac{\Gamma_2 \longrightarrow A, \Delta_2, A}{\overline{\Gamma_2 \longrightarrow \Delta_2, A}}$$

This construction gives a proof with fewer strong inferences than P and with the same endsequent as P which contradicts the minimality of P. $\square$

All of the theorems of this section also hold for the extension of PK to first-order logic. The proofs still work essentially without modification; the main new thing to check is that the constructions given above for removing strong inferences still yield valid proofs, and in particular, that the eigenvariable conditions are not violated. However, this is easily accomplished by assuming that the proofs are in free variable normal form, and this can be assumed without loss of generality since we are considering only tree-like proofs.

6 Cycles in the Logical Flow Graph

The logical flow graph of a proof P is a directed graph on occurences of subformulas in P indicating the 'implicational flow' of the formulas in the proof. The logical flow graph is defined in [4] and we do not repeat the definition here. (The reader who has never seen the definition of the logical flow graph might be able to figure out the definition from the two examples given below.)

Although [4] proves several nice properties of the logical flow graph, there are still many open problems about how complicated logical flow graphs need be. The first observation is that in a cut-free proof, the directed paths in the logical flow graph are very well behaved; namely, (1) for each positively occuring subformula A in the proof, there is a unique directed path leading from A to a subformula in the endsequent, and (2) for each negatively occuring formula B in the proof, there is a unique path leading from a subformula in the endsequent to B, and (3) every directed path consists of upward edges followed by downward edges (with a lateral edge at an initial sequent at the transition from upward edges to downward edges). To prove these three assertions, just note that since there are no cuts, a directed path can never have downward edges leading to a lateral edge followed by upward edges.

However, in the setting of general proofs with cuts, the situation is much more complicated; even in the simple case of propositional logic proofs. The general problem is to find 'normal form' properties of logical flow graphs that can be assumed to holds of logical flow graphs without superpolynomial proof size penalty. That is, to find nice properties $\mathcal{R}$ such that for any PK proof P, there is another PK-proof P' of the same endsequent such that the logical flow graph of P' enjoys property $\mathcal{R}$.

Of course the purpose of finding such properties $\mathcal{R}$ is (at least) twofold; namely, to give better methods on proving lower bounds on proof size and to give better heuristic algorithms for proof search.

One candidate for such a property $\mathcal{R}$ is the property of the logical flow graph being acyclic. Unfortunately this problem is open, even for propositional logic and even when allowing polynomial increase in proof size:

Question: If $\Gamma \longrightarrow \Delta$ has a PK-proof of strong inference length m, must it also have a PK-proof polynomial size (i.e., with $m^{O(1)}$ strong inferences) which has acyclic logical flow graph?

By an observation of Krajíček, it is enough to restrict one's attention to tree-like PK-proofs in answering this question, since every dag-like proof can be converted into a polynomial size tree-like proof.

Since it is somewhat surprising and counter-intuitive that tree-like PK-proof can have cycles, we give two examples below of tree-like proofs which are not acyclic. In both cases, the proofs are easily converted into much shorter proofs without cycles; but the point is that we asking whether every proof can be converted into a polynomial size proof with acyclic logical flow graph.

Example 1: In this example, the notations A^i indicate distinguished occurrences of the formula A. The logical flow graph contains an edge from A^i to A^{i+1} for all i except $i = 24$.[§] It also contains an edge from A^{24} to A^9 and an edge from A^{16} to A^{25}. Note that the nodes $A^9, A^{10}, A^{11}, \cdots, A^{24}, A^9$ form a cycle in the logical flow graph.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A^6 \longrightarrow A^7}{\neg A, A^5 \longrightarrow A^8, A} \quad \dfrac{\dfrac{A^{21} \longrightarrow A^{22}}{\longrightarrow A^{23}, \neg A^{20}}}{\neg A, A \longrightarrow A^{24}, \neg A^{19}}}{\neg A, A^4 \longrightarrow A^9, A \wedge \neg A^{18}} \quad \dfrac{\neg A^{28} \longrightarrow \neg A^{27}}{\neg A^{29}, A \longrightarrow \neg A^{26}, A \wedge \neg A}}{\neg A^{30}, A^3 \longrightarrow A^{10} \wedge \neg A^{25}, A \wedge \neg A^{17}}}{\neg A^{31}, A^2 \longrightarrow A^{11} \wedge \neg A^{16}} \quad \dfrac{\begin{array}{c}\ddots\ \vdots\ \iddots\\ A^{13}, \neg A^{14} \longrightarrow\end{array}}{A^{12} \wedge \neg A^{15} \longrightarrow}}{\neg A^{32}, A^1 \longrightarrow}$$

Example 2: The logical flow graph for the proof shown below contains directed edges from each occurrence B^i to B^{i+1} (there is no occurrence B^{27}). In addition, the logical flow graph contains a directed edge from B^{26} to B^9 and a directed edge from B^{12} to B^{28}. The nodes $B^9, B^{10}, B^{11}, \ldots, B^{26}, B^9$ form a cycle in the logical flow graph.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\begin{array}{c}\ddots\ \vdots\ \iddots\\ \longrightarrow \neg B^{21}, B^{22}\end{array}}{\neg B \longrightarrow \neg B^{20}, B^{23}} \quad \dfrac{\neg B^{33} \longrightarrow \neg B^{32}}{\neg B^{34} \longrightarrow \neg B, \neg B^{31}}}{\neg B^{35} \longrightarrow \neg B^{19}, B^{24} \wedge \neg B^{30}}}{\neg B^{36}, B \longrightarrow B^{25} \wedge \neg B^{29}, \neg B^{18}} \quad \dfrac{B^5 \longrightarrow B^6 \qquad \neg B^{16} \longrightarrow \neg B^{15}}{\neg B^{17}, B^4 \longrightarrow B^7 \wedge \neg B^{14}}}{\neg B^{37}, B^3 \longrightarrow B^{26} \wedge \neg B^{28}, B^8 \wedge \neg B^{13}}}{\neg B^{38}, B^2 \longrightarrow B^9 \wedge \neg B^{12}} \quad \begin{array}{c}\ddots\ \vdots\ \iddots\\ B^{10} \wedge \neg B^{11} \longrightarrow\end{array}}{\neg B^{39}, B^1 \longrightarrow}$$

[§]Since we have omitted some of the inferences from the proof figure, as indicated with double lines, some of the directed edges from A^i to A^{i+1} are not strictly speaking edges in the logical flow graph, but are only in the transitive closure of the logical flow graph.

7 Constant-depth Frege proofs

A recent important result on propositional proofs lengths is the theorem independently obtained by [14] and [13] which states that any constant depth Frege proof of the propositional pigeonhole principle requires exponentially many symbols (the constants in their exponential bounds depend on the depth of the Frege proof). Both [14] and [13] use the number of symbols in the Frege proofs only as a lower bound on the number of distinct subformulas of formulas in the proof. Since Theorem 4 above states that, w.l.o.g., the number of distinct subformulas in a Frege proof of the propositional pigeonhole principle is proportional to the number of lines in the proof, it follows immediately that there are exponential lower bounds on the number of lines in constant depth Frege proofs of the propositional pigeonhole principle.

In this section, we shall apply the notion of "active subformulas" to prove *any* family of constant depth Frege proofs with polynomially many lines can be translated into a family of constant depth Frege proofs of polynomially many symbols. Namely, we shall prove (see below for the definitions):

Theorem 13 *Suppose A is a tautology which is not an instance of a shorter tautology and that A has a depth d Frege proof of $\leq m$ lines. Also suppose that A contains at most $\leq m$ distinct literals. Then A also has a depth d Frege proof of $\leq 3 \cdot m^{d+1}$ symbols.*

We now define the syntax of formulas of proofs for constant depth Frege proofs. The logical connectives will be the unary negation ($\neg$) and an unbounded fanin OR ($\bigvee$). Formulas and their sizes and depths are inductively defined by:

(1) Any variable p is a formula of size 1 and depth 0. These are called *atomic* formulas.

(2) If A is a formula, then $\neg A$ is a formula. The size and depth of $\neg A$ are equal to the size and depth of A.

(3) If $X = \{A_1, \ldots, A_k\}$ is a finite set of formulas, then $\bigvee X$ is a formula. The depth of $\bigvee X$ is one plus the maximum depth of the A_i's. Its size is the sum of the sizes of the A_i's.

Note the the depth of a formula is equal to the depth of nesting of $\bigvee$'s, but that negations do not contribute to the depth. Also note that the size of the a formula is equal to the number of occurences of variables in the formula. For A and B formulas, we write $A \vee B$ as an abbreviation for $\bigvee\{A, B\}$. A *literal* is defined to be a formula of depth zero.

There are five rules of inference (including one axiom) for constant-depth Frege proofs which are given below. The first three rules are schematic rules where A, B and C maybe any variables; however, in the last three rules, X and Y represent arbitrary sets of formulas.

$$\text{Axiom:} \qquad \frac{}{A \vee \neg A}$$

$$\text{Weakening:} \qquad \frac{A}{A \vee B}$$

$$\text{Cut:} \qquad \frac{A \vee B \qquad (\neg A) \vee B}{B \vee C}$$

$$\text{Merging:} \qquad \frac{\bigvee X \vee \bigvee Y}{\bigvee(X \cup Y)}$$

$$\text{Unmerging:} \qquad \frac{\bigvee(X \cup Y)}{\bigvee X \vee \bigvee Y}$$

Although the last two rules of inference are not quite schematic in the sense defined in section 2, we can still meaningfully define the notion of "active subformula". The guiding principle is that a subformula occurence is active with respect to a given inference iff its principal connective is explicitly mentioned in the definition of the inference rule. Thus any axiom makes two subformula occurences active, any weakening inference makes one subformula occurence active, and any cut, merge or unmerge inference makes four subformula occurences active. It is easy to see that Lemma 1 also applies to our constant-depth Frege proofs. In particular, we also have:

Theorem 14 *Suppose A has an m line, constant depth Frege proof. Then there is a formula B such that $||B|| = O(m)$ and such that B also has an*

m-line constant depth Frege proof and such that A is a substitution instance of B. Furthermore, at most $c \cdot m$ distinct nonatomic subformulas occur in the proof of B, for c a constant. (In fact, $c = 3$ suffices.)

Proof The proof is as before: each nonatomic subformula of A which is not active anywhere in the constant-depth proof may be replaced everywhere by a new variable. The result is still a valid proof.

It is not difficult to see that the number of active subformulas at most $3m - 4$ if $m > 1$: this is because each inference introduces at most three new active subformulas, and because there are at least two axioms, which each introduce only one active subformula. □

We are now ready to prove Theorem 13. First, Theorem 14 tells us that A has a depth d proof P with at most $3m - 4$ distinct nonatomic subformulas. For $i \geq 0$ let α_i be the number of distinct subformulas of depth i in P. Clearly $\alpha_1 + \alpha_2 + \cdots + \alpha_d \leq 3m - 4$, and, by hypothesis, $\alpha_0 \leq m$. Let $\beta_0 = 1$ and, for $k > 0$, $\beta_k = \alpha_0 \prod_{i=1}^{k-1}(\alpha_i + 1)$. We claim that

(i) The size of any depth $k \geq 1$ formula in P is no greater than β_k.

(ii) The sum of the sizes of all distinct formulas of depth $< k$ occuring in P is no greater than β_k.

We prove this claim by induction on k. First note that any depth zero formula has size equal to 1. Now let's establish the claim for $k \geq 1$. Since a depth k formula consists of zero or more negations applied to $\bigvee X$ with X a set of formulas of depth $< k$, part (ii) of the claim implies part (i). Obviously, the sum of the sizes of all distinct depth $k-1$ formulas is bounded by α_{k-1} times the maximum size, β_{k-1}, of a depth $k-1$ formula. This plus the induction hypothesis giving an upper bound β_{k-1} on the total size of all depth $< k$ formulas yields the bound $\alpha_{k-1}\beta_{k-1} + \beta_{k-1} = \beta_k$ as desired.

From Claim (ii), Theorem 13 follows immediately; since the product $\prod_{i=1}^{d}(\alpha_i + 1)$ is bounded by $\left(\frac{3m-4}{d} + 1\right)^d$ which is always bounded by $3 \cdot m^d$.

8 The Renaming Rule

The renaming rule is a weak form of the substitution rule, which allows only variables to be substituted. We prove in this section that for Frege systems, the renaming rule is as powerful as the full substitution rule. (This theorem was first presented as a homework problem in [6].)

Definition A substitution σ is a *renaming substitution* if its range is contained in the set of propositional variables. A renaming inference is a substitution inference in which the substitution is a renaming substitution. Note that a renaming inference allows distinct variables to be identified since a renaming substitution is not required to be injective. A *renaming Frege system* consists of a Frege system augmented to allow renaming inferences.

A $\top/\bot$-substitution is a substitution with range contained in $\{\top, \bot\}$. (We assume w.l.o.g. that the nullary constants $\top$ and $\bot$ are in the propositional language.) A $\top/\bot$-substitution Frege proof system consists of a Frege system augmented with substitution inferences for $\top/\bot$ substitutions.

Theorem 15 *Renaming Frege systems p-simulate substitution Frege systems.*

Corollary 16 *Renaming Frege systems p-simulate extended Frege systems.*

Before proving the above theorem, we first prove the following lemma:

Lemma 17 $\top/\bot$ *Frege systems p-simulate substitution Frege systems.*

Proof (of lemma). It will suffice to show that a substitution inference that replaces occurrences of a variable p with a formula B can be succinctly simulated in a $\top/\bot$-substitution Frege proof. That is to say, from the hypothesis $A(p)$, we wish to infer $A(B)$ with a $\top/\bot$-substitution Frege proof.

To do this, first infer $A(\top)$ and $A(\bot)$ using two $\top/\bot$-substition inferences. Then derive, with no substitution inferences, the tautologies $B \wedge A(\top) \rightarrow A(B)$ and $\neg B \wedge A(\bot) \rightarrow A(B)$; these two derivations have number of lines linearly bounded by the number of connectives in $A(p)$ and with number of symbols quadratically bounded by the number of symbols in $A(p)$. From these four formulas, $A(B)$ follows tautologically in a constant number of inferences. □

Proof (of Theorem 15). By Lemma 17 it will suffice to prove a renaming Frege proof system can p-simulate a $\top/\bot$-substitution Frege proof. As usual, we can assume that both proof systems are based on the same underlying Frege proof system $\mathcal{F}$. We assume there is a $\top/\bot$-substitution Frege proof P of a formula $A(p_1, \ldots, p_n)$ and we must show that there is a renaming Frege proof of the same formula with size polynomially bounded by the size of P. (The *size* of a proof is defined to equal the number of symbols in the proof.)

The renaming proof of $A(\vec{p})$ proceeds as follows. We first give a Frege proof P_0 of $A(\top, \ldots, \top)$ which has size quadratically bounded by the size of A. This is possible since $A(\top, \ldots, \top)$ is a variable-free tautology; the Frege proof merely proves the true subformulas of $A(\top, \ldots, \top)$ and disproves its false subformulas. Similarly, we give a polynomial-size Frege proof P_1 of $A(\bot, \ldots, \bot)$.

Let $p_1, \ldots, p_m$ be the variables which occur in the proof P. Let Z be the formula

$$(p_1 \lor p_2 \lor \cdots \lor p_m) \land \neg(p_1 \land p_2 \land \cdots \land p_m)$$

which asserts that $p_1, \ldots p_m$ are not all true and are not all false. We shall prove there is a polynomial-size renaming Frege proof P_2 of the formula $Z \to A(\vec{p})$. To form P_2, begin by forming the sequence P' of formulas obtained by replacing each line $B(\vec{p})$ in P with the formula $Z \to B(\vec{p})$. P' will not be a valid proof, but it can be patched up to be a valid proof as follows. First, if $B(\vec{p})$ is inferred by a Frege inference in P, then $Z \to B(\vec{p})$ can be inferred by a constant number of Frege inferences from earlier lines in P'. Finally, consider a $\top/\bot$-substitution inference in P, say

$$\frac{B(p_i)}{B(\top)}$$

where we have suppressed the occurrences of the other variables in B. In P', the hypothesis and conclusion of the inference become $Z \to B(p_i)$ and $Z \to B(\top)$. To simulate this inference, first use $m-1$ renaming inferences to infer the formulas

$$Z(p_i/p_j) \to B(p_j)$$

for all $j \neq i$, from the hypothesis $Z \to B(p_i)$; here $Z(p_i/p_j)$ denotes the result of replacing p_i in Z with p_j. Then give proofs for the $m-1$ formulas

$p_j \wedge B(p_j) \to B(\top)$, each of which has size quadratically bounded by the size of B. From these $2n-2$ formulas, the formula $Z^{-i} \to B(\top)$ can easily be proved with $O(m^2)$ many inferences, where Z^{-i} is the formula

$$(p_1 \vee \cdots \vee p_{i-1} \vee p_{i+1} \vee \cdots \vee p_m) \wedge \neg(p_1 \wedge \cdots \wedge p_{i-1} \wedge p_{i+1} \wedge \cdots \wedge p_m).$$

(Note that each $Z(p_i/p_j)$ with $i \neq j$ is equivalent to Z^{-i}.) Now the only way that Z could be true and Z^{-i} false is for the variables $p_1, \ldots, p_m$ to have all the p_j's with $j \neq i$ assigned the same truth value and for p_i to have the opposite truth value. Thus, since $B(\top)$ is a tautology, an argument similar to the one used to show the existence of the proofs P_0 and P_1 shows that

$$Z \wedge \neg Z^{-i} \to B(\top)$$

has a polynomial-size Frege proof. From this and $Z^{-i} \to B(\top)$, the formula $Z \to B(\top)$ is derivable in a constant number of inferences.

A similar argument shows that the renaming rule can succinctly simulate inferences of the form

$$\frac{Z \to B(p_i)}{Z \to B(\bot)}.$$

In this way, P' is patched up to be a valid renaming Frege proof P_2 of $Z \to A(\vec{p})$.

Now it is easy to also see that

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_m) \wedge A(\top, \ldots, \top) \to A(\vec{p})$$

and

$$\neg(p_1 \vee p_2 \vee \cdots \vee p_m) \wedge A(\bot, \ldots, \bot) \to A(\vec{p})$$

have proofs with are polynomially bounded by the size of P. From these and from the proofs P_0, P_1 and P_2 we obtain a renaming Frege proof of $A(\vec{p})$ with only a constant number of further Frege inferences. □

It is interesting to note that the proof of Theorem 15 required the fact that $A(p)$ was a tautology in order to justify the existence of the proofs P_0 and P_1 of $A(\top, \ldots, \top)$ and $A(\bot, \ldots, \bot)$. Likewise, it also used the fact that any conclusion of a substitution rule is a tautology. Therefore, our proof does not apply to Frege systems enlarged with non-logical axioms; that is to say, with axioms which are not tautologies or with rules of inference that do not preserve validity.

References

[1] M. L. Bonet, *Number of symbols in Frege proofs with and without the deduction rule*, in Arithmetic, Proof Theory and Computational Complexity, P. Clote and J. Krajíček, eds., Oxford University Press, 1993, pp. 61–95.

[2] M. L. Bonet and S. R. Buss, *The deduction rule and linear and near-linear proof simulations*, Journal of Symbolic Logic, 58 (1993), pp. 688–709.

[3] S. R. Buss, *Polynomial size proofs of the propositional pigeonhole principle*, Journal of Symbolic Logic, 52 (1987), pp. 916–927.

[4] ——, *The undecidability of k-provability*, Annals of Pure and Applied Logic, 53 (1991), pp. 75–102.

[5] ——, *On Gödel's theorems on lengths of proofs II: Lower bounds for recognizing k symbol provability*, in Feasible Mathematics II, P. Clote and J. Remmel, eds., Birkhäuser-Boston, 1995, pp. 57–90.

[6] S. R. Buss and et al., *Weak formal systems and connections to computational complexity*. Student-written Lecture Notes for a Topics Course at U.C. Berkeley, January–May 1988.

[7] G. Cejtin and A. Čubarjan, *On some bounds to the lengths of logical proofs in classical propositional calculus* (russian), Trudy Vyčisl. Centra AN ArmSSR i Erevan. Univ., 8 (1975), pp. 57–64.

[8] S. A. Cook and R. A. Reckhow, *The relative efficiency of propositional proof systems*, Journal of Symbolic Logic, 44 (1979), pp. 36–50.

[9] M. Dowd, *Model-theoretic aspects of $P \neq NP$*. Typewritten manuscript, 1985.

[10] J. Krajíček, *On the number of steps in proofs*, Annals of Pure and Applied Logic, 41 (1989), pp. 153–178.

[11] ——, *Speed-up for propositional Frege systems via generalizations of proofs*, Commentationes Mathematicae Universitatis Carolinae, 30 (1989), pp. 137–140.

[12] J. Krajíček and P. Pudlák, *Propositional proof systems, the consistency of first-order theories and the complexity of computations*, Journal of Symbolic Logic, 54 (1989), pp. 1063–1079.

[13] J. Krajíček, P. Pudlák, and A. Woods, *Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle*, Random Structures and Algorithms, 7 (1995), pp. 15–39.

[14] T. Pitassi, P. Beame, and R. Impagliazzo, *Exponential lower bounds for the pigeonhole principle*, Computational Complexity, 3 (1993), pp. 97–140.

[15] R. A. Reckhow, *On the Lengths of Proofs in the Propositional Calculus*, PhD thesis, Department of Computer Science, University of Toronto, 1976. Technical Report #87.

[16] R. Statman, *Complexity of derivations from quantifier-free Horn formulae, mechanical introduction of explicit definitions, and refinement of completeness theorems*, in Logic Colloquium '76, R. Gandy and M. Hyland, eds., Amsterdam, 1977, North-Holland, pp. 505–517.

[17] G. Takeuti, *Proof Theory*, North-Holland, Amsterdam, 2nd ed., 1987.