Substitution and Propositional Proof Complexity

Sam Buss

Abstract We discuss substitution rules that allow the substitution of formulas for formula variables. A substitution rule was first introduced by Frege. More recently, substitution is studied in the setting of propositional logic. We state theorems of Urquhart's giving lower bounds on the number of steps in the substitution Frege system for propositional logic. We give the first superlinear lower bounds on the number of symbols in substitution Frege and multi-substitution Frege proofs.

> "The length of a proof ought not to be measured by the yard. It is easy to make a proof look short on paper by skipping over many links in the chain of inference and merely indicating large parts of it. Generally people are satisfied if every step in the proof is evidently correct, and this is permissable if one merely wishes to be persuaded that the proposition to be proved is true. But if it is a matter of gaining an insight into the nature of this 'being evident', this procedure does not suffice; we must put down all the intermediate steps, that the full light of consciousness may fall upon them." [G. Frege, *Grundgesetze*, 1893; translation by M. Furth]

1 Introduction

The present article concentrates on the substitution rule allowing the substitution of *formulas* for formula variables.[1] The substitution rule has long pedigree as it was a rule of inference in Frege's *Begriffsschrift* [9] and *Grundgesetze* [10], which contained the first in-depth formalization of logical foundations for mathematics. Since then, substitution has become much less important for the foundations of

Sam Buss
Department of Mathematics, University of California, San Diego, e-mail: sbuss@ucsd.edu,
Supported in part by Simons Foundation grant 578919.

[1] We do not concern ourselves with the much more common use of substitution allowing replacing (first-order) variables with terms.

mathematics, being subsumed by comprehension axioms. Indeed, substitution of formulas for formula variables, when it is even permitted, is generally viewed as being merely a derived rule of inference.

Interest in substitution rules was revived in the 1970's, however, by [5, 6, 21] working with propositional proof systems. Motivated by logical questions arising out of the P versus NP question, they were interested in the logical and computational strength of propositional proof systems (called "Frege systems") including propositional proof systems in which both modus ponens and substitution rule are allowed as inferences. In the propositional setting, if $\varphi(p)$ is a derived formula with p a propositional varible, then the substitution rule allows inferring $\varphi(\psi/p)$, namely by replacing every use of the variable p with the formula ψ.

The present article was instigated by the opportunity to write a contribution for a volume honoring Alasdair Urquhart. A large part of Urquhart's work concerns the proof complexity of propositional proof systems, especially relatively weak proof systems. Two of his papers give lower bounds for substitution Frege proof length. In addition, Urquhart's work also addresses Russell's use of substitution for the foundations of mathematics based on Russell's efforts to fix the paradoxes present in Frege's work. Quite apart from the inherent interest of the substitution rule, this makes it an appropriate topic for the present collection of papers.

Section 2 will briefly discuss the substitution rule in second-order logic. Substitution was used already in Frege's work introducing formal methods for mathematical reasons, encompassing both first- and second-order arithmetic. Section 2 discusses the well-known equivalence of substitution and comprehension in second-order logic, and touches very lightly on later attempts of Russell to use substitution as foundation for logicism.

Our principal interest in the substitution rule is in the setting of propositional logic, using the so-called Frege proof systems augmented with the substitution rule; this topic is discussed in Sections 3 and 4, which form the main parts of this paper. We are particularly interested in general bounds on the size of substitution Frege proofs. Section 3 gives the main definitions and discusses connections with substitution Frege systems and quantified propositional logic. It also discusses different forms of substitution including renaming substitution and $\top/\bot$-substitution. Section 4 states lower bounds on the number of inferences in substitution Frege proofs due to Urquhart; we extend these to obtain new lower bounds on symbol-length as well.

We thank Jeremy Avigad, Bruno Bentzen, Wojciech Dzik, and Alasdair Urquhart for very useful comments and feedback on an earlier draft of this paper.

2 Substitution in metamathematics

In preparing this article, I (the present author) took the opportunity to read the core work of Frege (in English translation) presented in his *Begriffsschrift* [9] and volume 1 of his *Grundgesetze* [10, 11]. This was a eye-opening experience. Although

it is at times hard to read Frege as his less formal, philosophical discussions do not always correspond exactly to his formal system, in the end, Frege gives more-or-less complete formal definitions, and overall, Frege's formulations of quantification theory are remarkably well-developed and advanced, and very clearly elucidated.[2] Frege's formal system encompasses both first-order and second-order logic. Frege's second-order objects are functions, defined in terms of their "course-of-values" or "value ranges" ("Werthverlauf"); this together with his Basic Law V provides a general comprehension axiom. Frege's pictograph representation of assertions may look awkward by modern standards when first encountered, but his proof system includes propositional logic and first- and second-order universal and existential quantifiers in a full and modern form. It even contains the sequent calculus as a special case.[3] Frege uses sophisticated methods for reasoning about inductive properties in a general way. He defines the non-negative integers in terms of equinumerous classes ("Gleichzahligkeit") starting in Section 38 of the *Grundgesetze* [10, 11]. The *Grundgesetze* also contains some rudimentary type theory in the sense of first- and second-level ("erster und zweiter Stufe") functions; however, for Frege, everything collapsed to the first-level functions. The notation, $\dot{\epsilon}$, used for defining a function in terms of its course-of-values is a precursor to lambda notation. Frege also used a definite article ("bestimmten Artikel") similar to Russell's upside-down iota symbol ι and a precursor to the Hilbert epsilon symbol. Furthermore, Frege used a formal method of introducing definitions, allowing the introduction of new pictographs to represent more complex formulas.

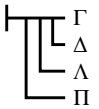
The substitution rule is given in Section 48 of the *Grundgesetze*, where it is presented as inference rule 9, allowing "Replacement of Roman letters" ("Ersatz der lateinische Buchstaben"). In short, it allowed any first-order function ("Funktion erster Stufe") to be substituted for a free variable as long as the number of argument places matched up. In the earlier *Begriffsschrift*, substitution is introduced without much fanfare or explanation starting in the derivation of (2) in Section 13. Later parts of the *Begriffsschrift* use increasingly strong substitution principles, culminating in derivations of (97), (98) and (110). (See Boolos [2], for more on the use of substitution in the *Begriffsschrift*.)

We can state a version of the substitution rule in modern terms as follows. We work in second-order logic. Unlike Frege, we use sets as second-order objects instead of functions. Let $F(x)$ be a second-order object; that is, $F(a)$ takes on Boolean values for arbitrary first-order objects a. Let $\Phi(x)$ and Ψ be an arbitrary second-order formulas.

---

[2] Indeed, Urquhart [27] mentions "Frege's limpid clarity", comparing it favorably with the work of Russell.

[3] The sequent calculus is included in the sense that a figure of the form (for instance)



corresponds to the sequent $\Pi, \Lambda, \Delta \rightarrow \Gamma$. The *Begriffsschrift* and *Grundgesetze* spend an unexpectedly long time discussing things that correspond to the structural rules, the cut rule and the negation rules of the sequent calculus.

We write $\Psi(\Phi/F)$ for the formula that results from replacing every instance $F(s)$ in Ψ with $\Phi(s/x)$, where $\Phi(s/x)$ means the formula obtained from Φ by replacing free occurrences of x with the term s.[4] The substitution rule allows us to infer

$$\frac{\Psi}{\Psi(\Phi/F)}$$

This form of the substitution rule is equivalent to comprehension; a fact first noticed by von Neumann [30] and again by Henkin [15]. The fact that substitution implies comprehension can be proved as follows (see [2]). Let $\Phi(x)$ be an arbitrary formula, and let A and X be unary predicate symbols. From the valid sequent $\exists X\,\forall x(X(x) \leftrightarrow A(x))$, we obtain $\exists X\,\forall x(X(x) \leftrightarrow \Phi(x))$ by substituting Φ for A. This is just the comprehension principle for Φ. The converse, that substitution follows from comprehension, is similarly easy to prove.

We hasten to add however that the substitution rule in the *Grundgesetze* was not as powerful as substitution in second-order logic; instead it served more as a convenience method to shorten proofs by being able to replace variables by arbitrary formulas. In particular, the substitution rule was not the mechanism used by Frege to establish comprehenson. That was done instead using course-of-values syntax and the Basic Law V of the *Grundgesetze*.

As is well known, the *Grundgesetze* proof system is inconsistent due to Russell's paradox. As Frege himself maintains in the appendix to volume 2 of [10], the Basic Law V is the problematic axiom. In fact, the problematic part is often referred to as "Basic Law Vb"[5], which we can restate in the language of second-order logic as

$$X = Y \;\rightarrow\; \forall x(X(x) \leftrightarrow Y(x)).$$

Stated in this form, Basic Law Vb presents as an instance of an equality axiom, and thus as completely unproblematic. However, it was a crucial axiom for the *Grundgesetze*. For Russell's paradox, one posits the existence of a the set of all sets which do not contain themselves as a member. In the *Grundgesetze*, and taking some liberties in notation, the property of a set a not being a member of itself is expressed as

$$(\exists b)(b = a \wedge a \notin b).$$

It requires the use of an equality axiom to conclude from this that $a \notin a$. My own take on this is that the real problem does not lie in Basic Law Vb. That law, stated as an equality axiom, seems completely true. Instead, the root cause of the inconsistency is the fact that the *Grundgesetze* system allows unresticted use of the course-of-values notation $\dot{\epsilon}$ to introduce functions.

Frege of course was devastated by Russell's paradox, and understood very clearly the problems it raised. He wrote in part,[6] "And even now I do not see how arithmetic

[4] The usual conditions on 'substitutability' must hold of course. These can always be enforced by renaming bound variables as necessary.

[5] See [10, §52].

[6] Translation by Furth of the appendix to volume 2 of the *Grundgesetze*.

can be scientifically founded, how numbers can be conceived as logical objects and brought under study, unless we are allowed—at least conditionally—the transition from a concept to its extension. Is it always permissable to speak of the extension of a concept, of a class? And if not, how do we recognize the exceptional cases?" [11, p. 127]

After discovering the paradoxes, Russell took up the effort of recasting Frege's theories into a consistent theory for the foundations of mathematics, including the foundations of arithmetic. He made a strong effort, in both published and unpublished works, to develop a "substitutional theory" in which substitution played a leading role. In those theories, the notation $p\frac{a}{x}!q$ indicated that the result of substituting x for every appearance of a in p yields q. This substitution notation was not just a syntactic construction; instead, "$p\frac{a}{x}!q$" served as a formula and indeed p, x, a, q could be quantified over as variables. Unfortunately, the substitutional theory also suffered from paradoxes, and Russell abandoned it favor of the type system of Whitehead and Russell's *Principia Mathematica*.

Russell's substitutional theory is not particularly relevant to the main topics of the present paper; nor is it not really about the syntactic operation of substitution. Furthermore, the present author is not particularly knowledgeable about it. We therefore do not consider it further. The interested reader is referred instead to Landini [19] and to the articles [12, 16, 20, 23, 27].

There is a great deal of work on Frege's formal systems for the foundations of mathematics. As a start, some that I have consulted include [1, 2, 13, 14, 31].

3 Substitution and propositional proofs

We now turn to the substitution rule in the setting of propositional proof systems. Propositional proof systems are much weaker than the second-order systems discussed above, but are still of more-than-considerable interest. A first reason for our interest is the connection to fundamental open questions in computational complexity such as the P versus NP question, or especially the NP versus coNP question, a connection first discovered by Cook [5]. A second reason is that propositional proof systems form the basis for many computerized verification and theorem-proving systems. Of course, a third reason is the intrinsic interest of the proof systems. The present section will discuss Frege proof systems, extended Frege proof systems, and several forms of substitution Frege proof systems. It will also explain the connection between the substitution rule and quantified propositional logic. The next section will discuss upper and lower bounds on the lengths of substitution Frege proofs.

A *propositional language* is a finite set L of propositional connectives, e.g., $L = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. We usually require that L is a complete set of Boolean connectives in that any Boolean function can be represented by an L-formula. A *propositional proof system* for L is a (total) polynomial time computable function f mapping $\{0,1\}^*$ onto the set of L-tautologies [6]. A traditional proof system P can be viewed as a propositional proof system by defining the function f_P so that when w

encodes a valid F-proof, $f_P(w)$ is equal to the formula proved by w, and for other w, $f_P(w)$ is equal to some arbitrary L-tautology.

We write $|w|$ and $|\varphi|$ to denote the length of a string w and a propositional formula φ. By "length" we mean the number of symbols in the string or formula. When P is a traditional proof in one of the inference systems defined below, and π is a P-proof, we write $|\pi|$ for the number of symbols in π, namely the sum of the lengths of the distinct formulas appearing in P. We call $|\pi|$ the *length* of π. The number of distinct formulas in π is called the *step length* of π. Since we only count distinct formulas, proofs are implicitly dag-like, not tree-like.

Suppose f and g are proof systems for L. We say that f *polynomially simulates* g provided there is a polynomial $p(n)$ so that for any g-proof w of a formula φ, there is an f-proof v of φ with $|v| \leq p(|w|)$. If $p(n)$ is linear, then we say f *linearly simulates* g. We call f and g *polynomially equivalent* if they polynomially simulate each other.

In propositional logic, the substitution rule is generally used as an augmentation of a Frege proof system. A Frege proof system is a propositional proof system with a finite number of axiom schemes and inference schemes which is implicationally sound and implicationally complete.[7] Without loss of generality, propositional formulas are formed using the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$ and $\leftrightarrow$ and the only inference rule is *modus ponens*. The finitely many axiom schemes typically include schemes such as $A \rightarrow (B \rightarrow A)$ where any formulas may be substituted for A and B. It is known that all Frege systems polynomially simulate each other [6], so the exact choice of connectives, axioms and inference rules is not particularly important. In addition, if two Frege systems use the same language, then they linearly simulate each other.

An *extended Frege proof* is allowed to use the *extension rule* [25] which permits inferring a formula

$$x \leftrightarrow C$$

where x is a new variable that does not appear in the formula C, or in the proof so far, or in the final line of the proof. The idea is that the new variable x serves as an abbreviation for the formula C. In principle, this may allow extended Frege proofs to be shorter than Frege proofs. However, it is open how much speedup of proof length extended Frege proofs provide over Frege proofs. This seems to be an extremely hard question, as it is related to the question of whether Boolean circuits can be represented by polynomial size formulas.

Definition 1 The *substitution rule* for Frege systems allows inferences of the form

$$\frac{A}{A(B/p)}$$

where the notation "$A(B/p)$" means the result of replacing every occurrence of the variable p in A with the formula B.

[7] We only briefly describe Frege proof systems here. For more background see Buss [4] or Krajicek [17].

The substitution rule is not implicationally sound since the hypothesis A may not logically imply the conclusion $A(B/p)$. However, it is sound, since the conclusion is valid whenever the hypothesis is valid.

The extension rule and substitution rule provide two ways to (apparently) add substantial strength to a Frege proof system. An *extended Frege* proof system is defined to be a Frege system augmented with the extension rule. Likewise, a *substitution Frege* proof system is a Frege proof system augmented with the substitution rule. It is common to use $\mathcal{F}$ to denote a particular Frege proof system. Then $e\mathcal{F}$ and $s\mathcal{F}$ denote the associated extended Frege and substitution Frege proof systems obtained by added the extension rule and the substitition rule (respectively) to $\mathcal{F}$.

It is also possible, although not nearly as common, to define a substitution rule that allows multiple substitutions in parallel.

Definition 2 The *multi-substitution rule* for Frege systems allows inferences of the form

$$\frac{A}{A(B_1/p_1, \ldots, B_k/p_k)} \tag{1}$$

where $p_1, \ldots, p_k$ are distinct variables, and where the notation "$A(B_1/p_1, \ldots, B_k/p_k)$" means the result of replacing every occurrence of each variable p_i in A with the formula B_i. The *multi-substitution Frege* proof system, $ms\mathcal{F}$, is obtained by adding the multi-substitution rule to a Frege system $\mathcal{F}$.

It is clear that a $s\mathcal{F}$-proof is also an $ms\mathcal{F}$-proof, so $ms\mathcal{F}$ trivially polynomially simulates $s\mathcal{F}$. Conversely, the action of a multi-substitution inference as shown above can be simulated by (at most) $2k-1$ substitution inferences. Namely, $k-1$ substitution inferences are used to replace $p_2, \ldots, p_k$ with new variables $p'_2, \ldots, p'_k$ and then k substitution inferences are used to replace $p_1, p'_2, \ldots, p'_k$ with $B_1, \ldots, B_k$. (The first $k-1$ inferences are used in case any p_j occurs in any B_i.) This shows that the (single) substitution Frege system $s\mathcal{F}$ polynomially simulates the multi-substitution system $ms\mathcal{F}$.

When working with a $s\mathcal{F}$ or $ms\mathcal{F}$ proof π, we can view the formulas in π as being implicitly universally quantified. That is, if a formula A has been proved in π, it means the same as $(\forall p)A$. Indeed, the substitution rule can be simulated in quantified propositional logic with the inferences

$$\text{modus ponens}\ \frac{\forall\text{-intro}\ \dfrac{A}{(\forall p)A} \qquad (\forall p)A \rightarrow A(B/p)}{A(B/p)}$$

The next theorem gives a central result about Frege systems.

Theorem 1 [6, 7, 18] *The extended Frege proof systems and substitution Frege proof systems are polynomially equivalent.*

It is open whether Frege systems can polynomially simulate the extended Frege and substitution Frege systems.

The fact that $s\mathcal{F}$ polynomially simulates $e\mathcal{F}$ systems as was proved by Cook and Reckhow [6], and we sketch the proof to give an example of the power of substitution.

Suppose π is an extended Frege proof of a formula A. Enumerate the uses of the extension rule in π as $x_i \leftrightarrow C_i$ for $i = 1, 2, \ldots, \ell$. We assume these extension axioms are given in the order in which they appear in π, and thus the condition that each x_i is a new variable implies that x_i does not appear in C_j for any $j < i$. Applying the deduction theorem ℓ times, there is a Frege proof of the formula

$$(x_\ell \leftrightarrow C_\ell) \to ((x_{\ell-1} \leftrightarrow C_{\ell-1}) \to (\cdots((x_2 \leftrightarrow C_2) \to ((x_1 \leftrightarrow C_1) \to A))\cdots)). \tag{2}$$

We use the substitution rule to replace x_ℓ with C_ℓ; note that x_ℓ does not appear anywhere in the formula (2) other than where it is indicated. We then prove the tautology $C_\ell \leftrightarrow C_\ell$ (with a proof of length polynomial in $|C_\ell|$), and use modus ponens to infer

$$(x_{\ell-1} \leftrightarrow C_{\ell-1}) \to (\cdots((x_2 \leftrightarrow C_2) \to ((x_1 \leftrightarrow C_1) \to A))\cdots).$$

This process is repeated $\ell - 1$ many more times until a derivation of A is obtained. This gives an $s\mathcal{F}$ proof of A with length polynomially bounded by the length of $|\pi|$.

The fact that $e\mathcal{F}$ polynomially simulates $s\mathcal{F}$ was proved by Dowd [7] in unpublished work, and then by Krajíček and Pudlák [18]. Dowd gave a proof based on proving the soundness of $s\mathcal{F}$ in the bounded arithmetic theory PV; Krajíček and Pudlák describe that proof in the setting of S^1_2, and also give an explicit simulation of $s\mathcal{F}$ by $e\mathcal{F}$. The reader should refer to [18] for details.

We conclude this section with two restrictions on the (multi-)substitution rule from [3] which have turned out to be as strong as unrestricted substitution. We henceforth assume that the language L contains the two constant symbols $\top$ and $\bot$ denoting the constants *True* and *False*, respectively.

Definition 3 A $\top/\bot$ *substitution inference* is a multi-substitution inference of the form (1) in which each formula B_i is either $\top$ or $\bot$.

Definition 4 A *variable renaming inference* is a multi-substitution inference of the form (1) in which each formula B_i is a variable.

Definition 5 A *permutation substitution inference* is a multi-substitution inference of the form (1) in which each B_i is a variable, and the mapping $p_i \mapsto B_i$ is a permutation of $\{p_1, \ldots, p_k\}$. It is permitted that some p_i's do not appear in A.

The difference between a variable renaming inference and a permutation substitution is that the former can replace two variables with the same variable. Namely, a variable renaming inference may have some B_i and B_j equal to each other, and thus the renaming inference causes the two variables p_i and p_j to be mapped to the same variable. This is not permitted in a permutation substitution inference. Since it may be that not all the p_i's actually appear in A, a permutation substitution inference should be viewed a permutation acting on all variables, not just on the variables appearing in A.

A $\top/\bot$-*substitution Frege* proof system is a Frege system augmented with the $\top/\bot$ substitution inference rule. A *renaming Frege* proof system is a Frege system

augmented with the variable renaming rule. These are known to be equivalent to (multi-)substitution Frege:

Theorem 2 [3] *$\top/\bot$-substitution Frege and renaming Frege are both polynomially equivalent to $s\mathcal{F}$ (and hence to $ms\mathcal{F}$ and $e\mathcal{F}$).*

However, it is open whether permutation Frege proof systems are polynomially equivalent to extended Frege systems. It is also open whether a Frege system can polynomially simulate a permutation Frege proof system.

4 Bounds on Substitution Frege proof length

This section discusses the best known lower bounds on the lengths and step lengths of substitution Frege proofs. This work was initiated by Urquhart [26, 28] who proved linear lower bounds on the step length of substitution Frege proofs. Urquhart was in turn motivated by results of Buss [3] giving a quadratic lower bound on the numbers of symbols in Frege proofs and extended Frege proofs for certain tautologies. Theorem 5 below gives new lower bounds on the lengths of (multi-)substitution Frege proofs. These kinds of lower bounds are of interest because of the connections between propositional proof length and the question of whether NP = coNP. In particular, if there exists a proof system P (in the sense of Cook and Reckhow) such that all tautologies have polynomial length P-proofs, then NP = coNP [6]. Thus, it is interesting to prove non-trivial lower bounds on proof length even for specific systems such as Frege, extended Frege, substitution Frege, etc.

For Frege and extended Frege systems we have (a weaker bound for Frege was proved earlier by [24]):

Theorem 3 [3] *There is an infinite family of tautologies φ_n for which the shortest extended Frege proofs have length $\Omega(|\varphi_n|^2)$. In addition, the shortest extended Frege proofs have step length $\Omega(|\varphi_n|)$.*

Of course this implies the same lower bounds for Frege proofs.

We henceforth make the (inessential) assumption that the propositional language contains the symbols $\top$, $\bot$, $\neg$, $\wedge$, $\vee$ and $\rightarrow$. The proof of Theorem 3 in [3] used formulas φ_n of the form

$$\bot \vee (\bot \vee (\bot \vee (\cdots (\bot \vee \top) \cdots))), \tag{3}$$

where there are n many $\bot$'s. Suppose π is an (extended) Frege proof of φ_n. A formula B appearing in π is defined to be *active* in π provided that there is an axiom or an inference in π which involves an occurrence of B, and the validity of the inference depends on the presence of the principal connective of B. For example, in an axiom $D \rightarrow (C \rightarrow D)$, the two formulas $D \rightarrow (C \rightarrow D)$ and $C \rightarrow D$ are active; however, C and D and their subformulas are not. Similarly, in a modus ponen inference inferring D from C and $C \rightarrow D$, only the formula $C \rightarrow D$ is active.

It is a simple observation, that if a formula B is not active in an (extended) Frege proof π, then the result of replacing every appearance of B in π uniformly with another formula B' results in a valid (extended) Frege proof π'. It follows that every subformula of φ_n must be active in π. This is because otherwise, we could replace that subformula by the constant $\bot$, thereby obtaining a valid proof of a false formula.

The proof of Theorem 3 is now almost immediate. An axiom or inference in π has only $O(1)$ many active formulas. Since every subformula of φ_n must be active in π, there must be $\Omega(n)$ many lines in π, so the step length of π is $\Omega(|\varphi_n|)$. Any active occurrence of a formula in π can be a subformula of only $O(1)$ many other occurrences of active formulas. Therefore, the number of symbols in π is bounded by $\Omega(s)$ where s is the sum of the sizes of the subformulas in φ_n. Clearly, $s \geq n^2$, so $|\pi| = \Omega(n^2) = \Omega(|\varphi_n|^2)$. This completes the proof sketch for Theorem 3.

Theorem 3 does not say anything about the lengths of substitution Frege proofs. In fact, the formulas φ_n have $s\mathcal{F}$-proofs of length $O(n)$ and step length. Urquhart [26, 28] addressed this by proving the following:

Theorem 4 *There are tautologies ψ_n such that any $ms\mathcal{F}$-proof of ψ_n requires step length $\Omega(n/\log n)$. There are tautologies χ_n such that any $s\mathcal{F}$-proof of χ_n requires step length $\Omega(n)$.*

The second part of Theorem 4 is proved in [28]. The formulas χ_n are formed by letting $n = 2^N$, and letting χ_n be a balanced conjunction of the formulas $p_i \to p_i$ for $i = 1, \ldots, n$. The $\Omega(n)$ lower bound is proved by extending the notion of "active" formulas to include also any formula B_i used in a (multi-)substitution inference (1), and then arguing that for every i, either p_i or $p_i \to p_i$ is active. As there can be only $O(1)$ many active formulas per inference in an $s\mathcal{F}$-proof, this gives the $\Omega(n)$ step length lower bound for $s\mathcal{F}$. This argument fails for $ms\mathcal{F}$-proofs however. Indeed, as Urquhart shows, there are $ms\mathcal{F}$-proofs of χ_n of step length $O(\log n)$.

The proof of the first part of Theorem 4, giving lower bounds on the step length of $ms\mathcal{F}$-proofs, uses formulas similar to, but more complicated than the φ_n's used for Theorem 3. The idea is to encode a binary string w into a propositional formula Ψ_w.

Inductively define Ψ_w for $w \in \{0,1\}^*$ as follows. For w the empty string, let Ψ_w equal just $\top$. Further let Ψ_{0w} be the formula $(\bot \vee \Psi_w)$, and let Ψ_{1w} be the formula $(\top \to \Psi_w)$. For instance, Ψ_{0101} is the formula

$$(\bot \vee (\top \to (\bot \vee (\top \to \top)))).$$

Urquhart [26] gives an information-theoretic/counting proof that there is a w of length n such that any $ms\mathcal{F}$-proof of Ψ_w requires step length $\Omega(n/\log n)$. The basic idea is to encode $ms\mathcal{F}$-proofs of step length m by a binary string of length $O(m \log m)$ using a "condensed detachment" inference — in essence this construction shows that an $ms\mathcal{F}$-proof can be specified by stating, for each line B in proof, what axiom or inference was used to derive B and which earlier lines (if any) were used as hypotheses for the inference deriving B. This description sets up a unification problem that can be solved to find the a "most general" desired proof. The end result gives a non-constructive proof that there are strings w such that Ψ_w requires $ms\mathcal{F}$-proofs of step

length $\Omega(n/\log n)$. For each n, ψ_n is set (non-constructively) be one of the Ψ_w's with $|w| = n$ that require $ms\mathcal{F}$-Frege proofs of step length $\Omega(n/\log n)$.

We now extend Theorem 4 to give a lower bound on the (symbol) length of $ms\mathcal{F}$-proofs.

Theorem 5 *There are tautologies ψ_n of length $|\psi_n| = \theta(n)$ such that any $ms\mathcal{F}$-proof of ψ_n has length $\Omega(n \log n)$.*

Theorem 5 will be proved using a version of Urquhart's formulas Ψ_w, together with an extension of the concept of "active" formula. First, we extend the notation Ψ_w somewhat, and let $\Psi_w \circ B$ denote the result of replacing the final $\top$ symbol in Ψ_w with the formula B. For w the empty string, $\Psi_w \circ B$ is just the formula B. Then, for any w, $\Psi_{0w} \circ B$ is $(\bot \vee \Psi_w \circ B)$ and $\Psi_{1w} \circ B$ is $(\top \to \Psi_w \circ B)$. Note that $\Psi_w \circ \top$ is the same as Ψ_w.

We also use the symbol "$\circ$" to denote string concatenation: for $v, w \in \{0,1\}^*$, $v \circ w$ denotes the concatenation of v and w. Clearly, $\Psi_v \circ (\Psi_w \circ B)$ is equal to $\Psi_{v \circ w} \circ B$. We write $v \sqsubseteq w$ to indicate that v is a substring of w. We write $w[i, j]$ for the substring of w starting with the $(i+1)^{\text{st}}$ symbol of w and ending with the j^{th} symbol of w. Thus $w[0, i]$ denotes the prefix of w containing the first i symbols of w; and $w[i, |w|]$ denotes the suffix of length $|w| - i$.

Before proving Theorem 5, we show the results are optimal for our Ψ_w formulas, by explicitly constructing $s\mathcal{F}$-proofs that have length $O(n \log n)$ and step length $O(n)$ for $n = |w|$. The $s\mathcal{F}$-proof proceeds by proving the tautologies

$$p \to (\Psi_v \circ p) \tag{4}$$

for longer and longer $v \sqsubseteq w$. First consider strings v of length one. Here $\Psi_0 \circ p$ is $(\bot \vee p)$ and $(\Psi_1 \circ p)$ is $(\top \to p)$, and the formulas

$$p \to (\bot \vee p) \qquad \text{and} \qquad p \to (\top \to p)$$

have constant size Frege proofs. For $|v| > 1$, express v as $v = u_1 \circ u_2$, where $|u_1| = \lceil \frac{1}{2}|v| \rceil$ and $|u_2| = \lfloor \frac{1}{2}|v| \rfloor$. Suppose that $p \to (\Psi_{u_1} \circ p)$ and $p \to (\Psi_{u_2} \circ p)$ have already been derived. From these, we derive

$$\dfrac{p \to (\Psi_{u_2} \circ p) \qquad \dfrac{p \to (\Psi_{u_1} \circ p) \qquad (\Psi_{u_2} \circ p) \to (\Psi_{u_1} \circ (\Psi_{u_2} \circ p))}{}\,\text{substitution}}{p \to (\Psi_{u_1} \circ (\Psi_{u_2} \circ p))}$$

The upper inference is a substitution replacing p with $(\Psi_{u_2} \circ p)$. The double line above the last step indicates that some steps (may) have been omitted. The last line follows tautologically as an instance of the rule "from $A \to B$ and $B \to C$ deduce $A \to C$". Since the Frege system is implicationally complete, this has a schematic derivation with $O(1)$ steps, and with $O(|v|)$ many symbols. Since $(\Psi_{u_1} \circ (\Psi_{u_2} \circ p))$ is the same as $(\Psi_v \circ p)$, this completes the desired derivation for $p \to (\Psi_v \circ p)$.

The final step of the $s\mathcal{F}$-proof applies substitution to $p \to (\Psi_w \circ p)$ to obtain $\top \to (\Psi_w \circ \top)$. From this, $\Psi_w \circ \top$ is derived with $O(1)$ more steps without further use of substitution. The $s\mathcal{F}$-proof does not need to prove the tautologies (4) for all v, only the ones that are needed to prove $p \to (\Psi_w \circ p)$. This gives a divide-and-conquer recursion. By inspection, the resulting $s\mathcal{F}$-proof has $O(n)$ many steps, and $O(n \log n)$ many symbols.

Theorem 5 will be proved using formulas Ψ_w. We just sketched how to form an $s\mathcal{F}$-proof of Ψ_w with length $O(|w| \log |w|)$ and step length $O(n)$. Thus, for these formulas at least, the length lower bound in Theorem 5 cannot be improved. However, the proof of Theorem 5 needs an additional assumption about w, since Ψ_w does have much shorter proofs for some w's. In particular, the formulas φ_n used for Theorem 3 have the form Ψ_{0^n}. For these formulas, the $s\mathcal{F}$-proofs just constructed have length $O(n)$ and step length $O(\log n)$. The reason for this shorter length and step length is that all the substrings v of w have the form 0^i, so there are only $O(\log n)$ many distinct tautologies $p \to (\Psi_v \circ p)$ needed for the $s\mathcal{F}$-proof of Ψ_0^n.

The needed additional assumption is that all the substrings v of w of length $K = \lceil 2 \log n \rceil$ are distinct. In other words, for $i \leq |w| - K$, the substrings $w[i, i+K]$ are distinct. It is easy to give a non-constructive proof of the existence of such a w; namely, a randomly chosen binary string w of length n has all its length K substrings distinct with probability approximately $\frac{1}{2}$. For $i < j$, the probability that two substrings of w, $w[i, i+K]$ and $w[j, j+K]$ are identical is equal to 2^{-K}. There are $\binom{n-K+1}{2} < n^2/2$ many ways to choose $i < j < n$. Thus, a union bound probability argument implies that most w's have all of their length K substrings distinct.[8]

Proof (of Theorem 5) Let $n > 0$ and $K = \lceil 2 \log n \rceil$. Let $w \in \{0,1\}^n$ such that all of w's length K substrings are distinct. Suppose π is a $ms\mathcal{F}$-proof of Ψ_w. The goal is to give a lower bound on the length of π. Recall the definition from [3] of "active occurrence" of a formula that was given above in the proof of Theorem 3. We shall modify that definition to define what it means for a Ψ_v to be "s-active" in π. The main point of "s-active" is to take into account substitution inferences in deciding what parts of what formulas are essential for the correctness of π as an $s\mathcal{F}$-proof. (This is different from Urquhart's notion of active formulas in $s\mathcal{F}$ proofs in [28].)

Let v be a substring of w. If one of the following situations hold, then we say Ψ_v is *s-active* in π. In each situation, we express v as a (non-trivial) concatenation $v = v_1 \circ v_2$.

(a) Suppose a substitution inference in π derives $A(B_1/p_1, \ldots, B_\ell/p_\ell)$ from A. Also suppose that for some $j \leq \ell$, A contains $\Psi_{v_1} \circ p_j$ as a subformula and that B_j has the form $\Psi_{v_2} \circ C$ for some v_2 and C. Further suppose that $v = v_1 \circ v_2$ and that neither v_1 nor v_2 is empty. Then Ψ_v is s-active in that inference and thus in π.

(b) Suppose that an inference I in π has an active occurrence of $\Psi_v \circ B$ for some B. Then Ψ_v is s-active in this inference and thus in π. Let v_2 be the maximal length

[8] A constructive way to find w with all length K substrings disjoint is as follows. Let $J = \lfloor \frac{1}{2} K \rfloor$. For $0 \leq i < n$, let $b_i \in \{0,1\}^J$ be the binary representation of the integer i padded with leading zeros as needed to make it have length J. Form the concatenation $b_0 \circ b_1 \circ b_2 \circ \cdots \circ b_{n-1}$. It can be shown that all length $2L$ substrings of w' are distinct. Let w be w' truncated to length n.

suffix of v such that $\Phi_{v_2} \circ B$ is not active in I (if such a v_2 exists). Then v_1 is the prefix of v such that $v = v_1 \circ v_2$.

In situation (b), we wish to have v_2 exist and be non-empty. This can be arranged by noting that for any particular Frege system $\mathcal{F}$, there is an upper bound K_0 on the length of v_1. This is because the Frege system is schematic, and the finitely many axiom schemes and inference schemes only nest connectives to a fixed depth. (In fact, we can take K_0 equal to 2 in the most common axiomatization for Frege systems.) We shall only consider whether Ψ_v is s-active when $|v| > K_0$. Then, when Ψ_v is s-active due to condition (b) holding for an active occurrence of $\Psi_b \circ B$, it must be that $|v_1| \leq K_0$ and hence that v_2 is non-empty.

The condition $|v| > K_0$ will automatically be satisfied in our construction below if $K + K_0 \leq K^2$; this holds for n sufficiently large. In fact, $n \geq 2$ will suffice if $K_0 = 2$.

Lemma 1 *Let π be an $ms\mathcal{F}$-proof of Ψ_w and suppose $v \sqsubseteq w$ is non-empty. Then Ψ_v must be s-active in π.* □

Proof Suppose for sake of contradiction, that Ψ_v is not s-active in π. We shall modify π so that it remains a syntactically correct $ms\mathcal{F}$ proof, but ends with a formula which is not a tautology. This will be a contradiction.

Modify π as follows. Let v' be the substring of v containing all but the first symbol of v. Find every occurrence in π of a subformula of the form $\Psi_v \circ B$. Such a subformula has one of the forms $(\bot \vee (\Psi_{v'} \circ B))$ or $(\top \rightarrow (\Psi_{v'} \circ B))$ depending on whether v's first symbol is a 0 or a 1. In either event, replace this formula with

$$(\bot \wedge (\Psi_{v'} \circ B)).$$

By inspection, the transformed π remains a correct $ms\mathcal{F}$ proof after this transformation, since otherwise Ψ_v would have been s-active in π. And, the final line, $\Psi_w \circ \top$, has been transformed into a false formula because of the presence of "$(\bot \wedge \cdots)$" in the transformed $\Psi_w \circ \top$. This gives the desired contradiction. □

The proof of Theorem 5 will be based on a dynamic process searching for a v with $|v| \geq K^2$ such that Ψ_v is not s-active in the given proof π. Of course, by the lemma, there is no such v. However, the process of searching for an non-s-active v will identify appearances of formulas $\Psi_v \circ B$ in π which jointly contain $\Omega(n \log n)$ symbols. The search process will maintain two sets, Q and P, of strings $v \sqsubseteq w$: strings in Q are called "queued" and strings in P are called "processed". Initially, Q contains only w, and P is empty. Strings in Q will be processed one at a time, and then moved to P, possibly adding additional strings to Q. The following two invariants i. and ii. will be maintained throughout the process.

i. The strings in Q all have length at least K^2 and are substrings of w. Since $K^2 \geq K$, this means each $v \in Q$ corresponds to a unique substring location in w, namely v can be uniquely expressed as $v = w[i, j]$ (with $j = i + |v|$). We call this the "w-location" of v. The w-locations of the queued v's are disjoint (non-overlapping) substrings of w.

ii. Each substring v in P will have earlier been in Q; hence $|v| \geq K^2$ and $v \sqsubseteq w$. For any $v_1 \neq v_2 \in P$, one the following holds: (a) $v_1 \sqsubseteq v_2$, (b) $v_2 \sqsubseteq v_1$, or (c) the w-locations of v_1 and v_2 are disjoint substrings of w. Furthermore, each $v \in P$ will be associated with an occurrence of a subformula $\sigma(v)$ somewhere in π. The subformula $\sigma(v)$ will have the form $\Psi_v \circ B$.

The process runs as follows. Pick an arbitrary $v \in Q$. By Lemma 1, v must be s-active in π. This means that at least one of the following situations hold. It may be that there are multiple ways that (a) and (b) hold; but in this case, the process just picks arbitrarily one way they hold, so that v gets processed and put into P only once.

(a) Case (a) of the definition of s-active holds for Ψ_v. There are v_1 and v_2 such that $v = v_1 \circ v_2$ and a substitution inference deriving the formula $A(B_1/p_1, \ldots, B_k/p_k)$ from A. The formula A contains a subformula $\Psi_{v_1} \circ p_j$ and B_j has the form $\Psi_{v_2} \circ C$. This introduces a new subformula of the form $\Psi_v \circ C$. We move v from Q to P, and let $\sigma(v)$ equal one of the subformulas $\Psi_v \circ C$ introduced in D by the substitution of B_j for p_j. We add v_1 and v_2 to Q unless they have length $< K^2$.

(b) Case (b) of the definition of s-active holds for Ψ_v. There is an inference I in π in which $\Psi_v \circ B$ is active. For such an I and active occurrence of $\Psi_v \circ B$, we can express v as $v = v_1 \circ v_2$ where $|v_1| \leq K_0$ and v_2 is the maximal suffix of v such that $\Psi_{v_2} \circ B$ is not active in the inference I. If there is more than one way to choose I and an active occurrence of a formula $\Psi_v \circ B$, then choose them so as to maximize the length of v_1. We move v from Q into P, and let the associated formula $\sigma(v)$ be the chosen active occurrence of $\Psi_v \circ B$. We add v_2 to Q if it has length $\geq K^2$. Since $|v_1| \leq K_0 < K^2$ (for n sufficiently large), v_1 is not added to Q.

The process stops when Q becomes empty.

It is not hard to see that the invariants i. and ii. hold throughout the process. Every v in P or Q has length $K^2 > K$ and thus has a unique w-location as $v = w[i, j]$. Since the process acts by splitting strings v into two substrings as $v = v_1 \circ v_2$, moving v to P and possibly adding v_1 and v_2 to Q, it is clear that invariants i. and ii. hold.

To finish the proof of Theorem 5, we shall show that the subformulas $\sigma(v)$ for $v \in P$ contribute $\Omega(n \log n)$ symbols to the length of π.

It is helpful to view strings in P as being vertices of a tree in which each node has degree at most 2. The node w is the root, since w is the first string put in Q, and thus the first string put in P. And, if $v \in P$, the children (if any) of v are the $\sqsubseteq$-maximal $v' \in P$ such that $v' \sqsubset v$. Namely, v' is a child of v iff $v' \sqsubset v$ and there is no $v'' \in P$ such that $v' \sqsubset v'' \sqsubset v$. The uniqueness of the w-locations, the invariant ii., and the fact that the process always splits strings v into at most two substrings means this gives a tree in which each node has at most two children. Any v in P which is a leaf vertex has length $|v| < 2K^2 - 1$; otherwise, either case (a) or (b) would act to give at least one child of v.

A $v \in P$ will called "type (a)" or "type (b)" depending whether the process used case (a) or case (b) to add v to P.

It would be nice if we could argue that the subformulas $\sigma(v)$ for $v \in P$ were all disjoint and non-overlapping; however, we have not been able to do this. Instead

we will show three things: First, Lemma 2 will limit how much the w-locations of any two v's in P of type (a) can overlap, and thereby identify a way to avoid double-counting symbols in the formulas $\sigma(v)$ for v's of type (a). Second, Lemma 3 will show that the subformulas $\sigma(v)$ for $v \in P$ of type (b) are disjoint and do not overlap. Third, Lemma 4 shows that for $v \in P$ of type (a), $\sigma(v)$ overlaps with $\sigma(v')$ for at most one $v' \in P$ of type (b).

For $v \in P$, the formula $\sigma(v)$ has the form $\Psi_v \circ B$ for some B. The first $|v|$ binary connectives are $\vee$'s and $\rightarrow$'s according to the symbols 0 and 1 in v. We call these the *top binary connectives* of $\sigma(v)$. The terminology "top" is since we think of the formula $\sigma(v)$ as a tree with root at the top: the "top" part is the part above B. There are $|v|$ many top binary connectives in $\sigma(v)$.

Lemma 2 *Suppose $v \neq v' \in P$ and both v and v' are type (a). Then the subformulas $\sigma(v)$ and $\sigma(v')$ have less than K top binary connectives $\vee$ and $\rightarrow$ in common.* □

Because of the linear (non-branching) structure of the formula Ψ_v and $\Psi_{v'}$, Lemma 2 means that the overlapping top binary connectives of $\sigma(v)$ and $\sigma(v')$ are connectives corresponding to the right end of v and the left end of v', or vice-versa. Our lower bound on the length of the $ms\mathcal{F}$-proof π will be obtained by arguing that each $v \in P$ contributes $\geq |v| - K$ many symbols to π (subject to the multiplicative reduction required by the next two lemmas).

Proof (of Lemma 2) Suppose $\sigma(v)$ and $\sigma(v')$ contain K or more top binary connectives ($\vee$'s and $\rightarrow$'s) in common. These are formulas $\Psi_v \circ B$ and $\Psi_{v'} \circ B'$. Without loss of generality, $\sigma(v')$ is a subformula of $\sigma(v)$. Therefore, one of the following situations hold: (1) $v' \sqsubset v$ and $v = u_1 \circ v' \circ u_3$ for some u_1, u_3, or (2) $v = u_1 \circ u_2$ and $v' = u_2 \circ u_3$ for some u_1, u_2, u_3 with u_2 non-empty.

We claim that case (1), $v' \sqsubset v$, is impossible. Since v is type (a), the process found a multi-substitution inference J, and v_1 and v_2, such that $v = v_1 \circ v_2$ and the multi-substitution inference created $\Psi_{v_1 \circ v_2} \circ B = \Psi_v \circ B$ by substituting $\Psi_{v_2} \circ B$ for a variable p_j. Exactly the same holds for v' for some substrings v'_1 and v'_2 of v', with the *same* substitution inference J. (This is because $\sigma(v)$ and $\sigma(v')$ overlap and are both type (a).) Since $v' \sqsubset v$, the tree properties for the strings in P means that either $v' \sqsubseteq v_1$ or $v' \sqsubseteq v_2$. As $\sigma(v')$ is a subformula of $\sigma(v)$, this means that it is impossible for the same multi-substitution inference to have been used to process both v and v', as the decomposition $v = v_1 \circ v_2$ would have to split v somewhere outside of v', and the decomposition $v' = v'_1 \circ v'_2$ has to do the split inside v'.

Now consider case (2), $v = u_1 \circ u_2$ and $v' = u_2 \circ u_3$. The invariant ii. implies that the w-locations for v and v' are disjoint. The fact that there are no repeated substrings of length K in w thus means that $|u_2| < K$, so v and v' overlap in $< K$ symbols. Thus $\sigma(v)$ and $\sigma(v')$ have $< K$ top binary connectives in common. □

Lemma 3 *Let v and v' be of type (b) in P. Then $\sigma(v)$ and $\sigma(v')$ are disjoint subformulas in π.* □

Proof Suppose $\sigma(v)$ and $\sigma(v')$ not disjoint, Because of the "linear" structure of the formulas Ψ_v and Ψ'_v, one of $\sigma(v)$ and $\sigma(v')$ is a subformula of the other. The strings

v and v' were processed using case (b), using inferences I and I', respectively, and expressing $v = v_1 \circ v_2$ and $v' = v'_1 \circ v'_2$ and finding active formulas $\Psi_{v_1} \circ \Psi_{v_2} \circ B$ and $\Psi_{v'_1} \circ \Psi_{v'_2} \circ B'$. By the fact that we choose I and I' and the active formulas $\Psi_{v_1} \circ \Psi_{v_2} \circ B$ and $\Psi_{v'_1} \circ \Psi_{v'_2} \circ B'$ so as to maximize $|v_1|$ and $|v'_1|$, it must be that $\Psi_{v_2} \circ B$ and $\Psi_{v'_2} \circ B'$ are maximal non-active subformulas and thus are are exactly the same subformula. (In fact, we may assume that I and I' are the same inference.) Thus, either v_2 is a prefix of v'_2 or vice-versa.

From $|v_1|, |v'_1| \leq K_0$ and $|v|, |v'| \geq K^2$, we have that both $|v_2|$ and $|v'_2|$ are $\geq K^2 - K_0 \geq K$. So v and v' share a common substring of length $\geq K$. Hence their w-locations overlap, and by the tree properties for members of P, either $v \sqsubset v'$ or $v' \sqsubset v$. W.l.o.g., $v' \sqsubset v$. Since v is type (b), v_1 did not get added to Q, so $v' \sqsubseteq v_2$.

We have $|v'| \leq |v_2|$ and $|v'_1| \geq 1$; thus $|v'_2| < |v_2|$ and v'_2 is a proper prefix of v_2. Recall however that $|v'_2| \geq K$. This means that v'_2 appears at two places in v_2 as a substring: once since v'_2 is a prefix of v_2, and once since $v' = v'_1 \circ v'_2 \sqsubseteq v_2$. (Possibly the places overlap.) This violates the uniqueness property for w-locations for strings of length K. □

Lemma 4 *Suppose $v \in P$ is type (a). Then $\sigma(v)$ overlaps with $\sigma(v')$ for at most one v' of type (b).* □

Proof Suppose $v, v', v'' \in P$ have types (a), (b) and (b), respectively; also suppose $\sigma(v)$ overlaps with both $\sigma(v')$ and $\sigma(v'')$. Now $\sigma(v)$ has the form $\Psi_v \circ C$, and $|v| \geq K^2 > K_0$. Each of $\sigma(v')$ and $\sigma(v'')$, must either contain $\sigma(v)$ or be nested no more than K_0 levels deep inside $\sigma(v)$. Because of the "linear" structure of Ψ_v, this implies that $\sigma(v')$ must overlap with $\sigma(v'')$, contradicting Lemma 3. □

Based on three lemmas, we can lower bound the number of connectives $\vee$ and $\rightarrow$ appearing in π by

$$\frac{1}{2} \sum_{v \in P} (|v| - K).$$

This counts all but the K topmost (leftmost) top binary connectives in $\sigma(v)$ for $v \in P$. By Lemma 2, this avoids double counting symbols in $\sigma(v)$'s with v of type (a). The multiplicative factor of $\frac{1}{2}$ takes into account Lemma 4 so that we do not double count connectives that appear both in a $\sigma(v)$ and a $\sigma(v')$ with v of type (a) and v' of type (b).

To finish the proof of Theorem 5 it suffices to prove that $\sum_{v \in P}(|v| - K)$ is $\Omega(n \log n)$. This is a straightforward, albeit a bit detailed, computation, which we now carry out. Let

$$f(m) \;=\; m \log(m/K^3) + K,$$

where the logarithm is base 2. Recall that $K = \lceil 2 \log n \rceil$.

Lemma 5 *For $v \in P$, let P_v be the set $\{v' \in P : v' \sqsubseteq v\}$. Then*

$$f(|v|) \;\leq\; \sum_{v' \in P_v} (|v'| - K). \tag{5}$$

Note that P_v is the set of strings v' in the subtree rooted at v.

Proof We may assume n is sufficiently large. In particular, it is convenient to require at least $n \geq 4$ and $K \geq 4$, and $K^2 \geq K + K_0$. The proof is by induction on $m = |v|$. First suppose v is a leaf in the tree of members of P. Since v is a leaf member of P, we have $K^2 \leq m < 2K^2$. In fact, we need only that $K^2 \leq m \leq K^3$. Since $P_v = \{v\}$, the inequality (5) becomes

$$m \log(m/K^3) + K \;\leq\; m - K. \tag{6}$$

From $m \leq K^3$, we have $\log(m/K^3) \leq 0$, so it will suffice to show $K \leq m - K$. This holds as $m \geq K^2 \geq 2K$.

There are two induction cases to consider. The first is when v has two children v_1 and v_2 in P (with $|v_1|, |v_2| \geq K^2$). Let $m_1 = |v_1|$ and $m_2 = |v_2|$, so $m = m_1 + m_2$. Since P_v is the union of $\{v\}$, P_{v_1} and P_{v_2}, and by the induction hypothesis applied to v_1 and v_2, it suffices to show that

$$f(m) \;\leq\; (m - K) + f(m_1) + f(m_2). \tag{7}$$

We claim that $f(m)$ is concave up. This is easy to check by noting that the first derivative

$$f'(m) \;=\; \log(m/K^3) + 1, \tag{8}$$

is an increasing function. Therefore, by convexity and since $m_1 + m_2 = m$, it suffices to prove that $f(m) \leq (m - K) + 2f(m/2)$. In other words,

$$m \log(m/K^3) + K \;\leq\; (m - K) + 2\Big(\frac{m}{2} \log(m/2K^3) + K\Big).$$

In fact, the two sides are equal.

The other induction step is when v has a single child. This arises in case (b), and also in case (a) when v_1 or v_2 has length $< K^2$. Let's assume $|v_1| < K^2$; the other case is dual. We have $m_1 = |v_1| < K^2$ and $m_2 = m - m_1 > m - K^2$, and P_v is $\{v\} \cup P_{v_2}$. If $m \leq K^3$, the desired inequality (5) follows from (6); recall that (6) was proved using only the hypothesis $K^2 \leq m \leq K^3$. So we may assume $m > K^3$. By the induction hypothesis for v_2 it suffices to show

$$f(m) \;\leq\; (m - K) + f(m_2). \tag{9}$$

We claim that the derivative (8) is positive for $m \geq K^3 - K^2$. To see this, note that $(K^3 - K^2)/K^3 \geq 3/4$ since $K \geq 4$, so for $m \geq K^3 - K^2$, we have $\log m/K^3 > -1$. Therefore, to establish (9), it suffices to show

$$f(m) \;\leq\; (m - K) + f(m - K^2).$$

since $m_2 \geq m - K^2$. In other words,

$$m(\log m - \log K^3) + K \;\leq\; m - K + (m - K^2)(\log(m - K^2) - \log K^3) + K.$$

We have $\log m - \log(m - K^2) \leq (K^2/(m - K^2))/\ln 2 \leq \frac{3}{2}(K^2/(m - K^2))$ from a first-order approximation to $\log x$ at $x = m - K^2$. So, regrouping and cancelling terms, it will suffice to show

$$K^2 \log(m - K^2) + K \;\leq\; m\Big(1 - \frac{3K^2}{2(m - K^2)}\Big) + K^2 \log K^3,$$

With $m \geq K^3$ and $K \geq 4$, we have $\frac{3}{2}(K^2/(m - K^2)) \leq 1/2$, so it will further suffice to show

$$K^2 \log m + K \;\leq\; \frac{m}{2} + K^2 \log K^3, \tag{10}$$

When we set $m = K^3$ in (10), it becomes, after cancellation, $K \leq K^3/2$. So (10) holds for $m = K^3$. To handle $m > K^3$, let LHS and RHS be the left- and righthand sides of (10). Their derivatives are

$$\frac{\partial}{\partial m}(\text{LHS}) = \frac{K^2}{m} \qquad \text{and} \qquad \frac{\partial}{\partial m}(\text{RHS}) = \frac{1}{2}.$$

Thus, $\frac{\partial}{\partial m}(\text{LHS}) \leq \frac{\partial}{\partial m}(\text{RHS})$ for $m \geq K^3$, since $K \geq 2$. It follows that (10) holds for all $m \geq K^3$. That proves Lemma 5. □

We can now finish the proof of Theorem 5. We have Ψ_w is a tautology of length $n = |w|$. Any $ms\mathcal{F}$-proof of Ψ_w must have at least $\frac{1}{2}f(n)$ many occurrences of binary connectives. Furthermore, since $K = \lceil 2 \log n \rceil$,

$$f(n) \;=\; n \log n - n \log K^3 + K$$

has growth rate $\Omega(n \log n)$. □

Theorem 5 bounds the length of $ms\mathcal{F}$ proofs with length measured as the number of symbols in the proof. Urquhart's theorem gives a $\Omega(n/\log n)$ lower bound on the number of steps in an sF-proof of (a randomly chosen version of) the same formulas. We conjecture that for suitable w of length n, the correct lower bound for the step length of an $s\mathcal{F}$-proof of Ψ_w is $\Omega(n)$. In fact, we even conjecture an $\Omega(n)$ lower bound for the step length of $ms\mathcal{F}$-proofs of these formulas.

Of course, if the commonly accepted conjectures about NP are true, then there are formulas that require exponential size $ms\mathcal{F}$-proofs. But obtaining such lower bounds is at present well out of reach.

References

1. B. Bentzen, *Frege's theory of types*. https://arxiv.org/abs/2006.16453, 2020.
2. G. Boolos, *Reading the Begriffschrift*, Mind, (New series) 94 (1985), pp. 331–344.
3. S. R. Buss, *Some remarks on lengths of propositional proofs*, Archive for Mathematical Logic, 34 (1995), pp. 377–394.

4. ———, *Propositional proof complexity: An introduction*, in Computational Logic, U. Berger and H. Schwichtenberg, eds., Springer-Verlag, Berlin, 1999, pp. 127–178.
5. S. A. Cook, *Feasibly constructive proofs and the propositional calculus*, in Proceedings of the Seventh Annual ACM Symposium on Theory of Computing, Association for Computing Machinery, 1975, pp. 83–97.
6. S. A. Cook and R. A. Reckhow, *The relative efficiency of propositional proof systems*, Journal of Symbolic Logic, 44 (1979), pp. 36–50.
7. M. Dowd, *Model-theoretic aspects of $P \neq NP$*. Typewritten manuscript, 1985.
8. P. A. Ebert and M. Rossberg, *Basic Laws of Arithmetic*, Oxford University Press, 2013.
9. G. Frege, *Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens*, Halle, 1879. English translation by Stefan Bauer-MengelBerg, with an introduction by van Heijenoort, in [29], pages 1-82.
10. ———, *Grundgesetze der Arithmetik*, Verlag Hermann Pohle, 1893/1903. Two volumes. English translation in [8]; partial translation of volume 1 in [11].
11. M. Furth, *The Basic Laws of Arithmetic*, University of California Press, 1964.
12. I. Grattan-Guiness, *The Russell archives: Some new light on Russell's logicism*, Annals of Science, 31 (1974), pp. 387–406.
13. R. G. Heck, *Frege's Theorem*, Oxford University Press, 2011.
14. ———, *Reading Frege's Grundgesetze*, Oxford University Press, 2012.
15. L. Henkin, *Banishing the rule of substitution for functional variables*, Journal of Symbolic Logic, 18 (1953), pp. 201–208.
16. P. Hylton, *Russell's substitutional theory*, Synthese, 45 (1980), pp. 1–31.
17. J. Krajíček, *Proof Complexity*, Cambridge University Press, 2019.
18. 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.
19. G. Landini, *Russell's Hidden Substitutional Theory*, Oxford University Press, 1998.
20. J. Pelham and A. Urquhart, *Russellian propositions*, in Proc. Logic, Methodology and Philosophy of Science IX, Studies in Logic and Foundations of Mathematics 134, Elsevier, 1995, pp. 307–326.
21. 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.
22. J. Siekmann and G. Wrightson, *Automation of Reasoning*, vol. 1&2, Springer-Verlag, Berlin, 1983.
23. G. Stevens, *Substitution and the theory of types: Review of* Landini, "Russell's Hidden Substitutional Theory", Russell, The Journal of Bertrand Russell Studies, 23 (2003), pp. 161–176.
24. G. Tseitin and A. Choubarian, *On some bounds to the lengths of logical proofs in classical propositional calculus* (Russian), Trudy Vyčisl. Centra AN ArmSSR i Erevanskovo Univ., 8 (1975), pp. 57–64.
25. G. S. Tsejtin, *On the complexity of derivation in propositional logic*, Studies in Constructive Mathematics and Mathematical Logic, 2 (1968), pp. 115–125. Reprinted in: [22, vol 2], pp. 466-483.
26. A. Urquhart, *The number of lines in Frege proofs with substitution*, Archive for Mathematical Logic, 37 (1997), pp. 15–19.
27. ———, *Review of* G. Landini, "Russell's Hidden Substitutional Theory", Journal of Symbolic Logic, 64 (1999), pp. 1370–1371.
28. ———, *The complexity of propositional proofs with the substitution rule*, Logic Journal of the IGPL, 13 (2005), pp. 287–291.
29. J. van Heijenoort, ed., *From Frege to Gödel: A Source Book in Mathematical Logic, 1879-1931*, Harvard University Press, 1967.
30. J. von Neumann, *Zur Hibertschen Beweistheorie*, Mathematische Zeitschrift, 26 (1927), pp. 1–46.
31. E. N. Zalta, *Frege's theorem and foundations for arithmetic*. Stanford Encylopedia of Philosophy, https://plato.stanford.edu/entries/frege-theorem, 1998, revised 2018. Retrieved July 26, 2020.