Number of Symbols in Frege Proofs with and without the Deduction Rule

Maria Luisa Bonet*
Department of Mathematics
University of California, San Diego

May 9, 2004

Abstract

Frege systems with the deduction rule produce at most quadratic speedup over Frege systems using as a measure of length the number of symbols in the proof. We study whether that speedup is in reality smaller. We show that the speedup is linear when the Frege proofs are tree-like. Also, two groups of formulas, permutation formulas and transitive closure formulas, that seemed most likely to produce an almost quadratic speedup when using the deduction rule, are shown to produce only $\log n$ and $\log^2 n$ factors respectively.

1 Introduction

A Frege proof system is an inference system for propositional logic in which the only rule of inference is Modus Ponens.

Definition 1 *A Frege Proof System consists of:*

1. *A finite complete set of propositional connectives. We use the following set:* $\neg, \vee, \wedge, \supset$.

*Supported in part by NSF Grant DMS-8902480.

2. *A finite set of axiom schemata.*

3. *A proof in this system is a sequence of lines $A_1, \ldots, A_n$ where each A_i is either a substitution instance of an axiom scheme, or is inferred by Modus Ponens(MP) from some formulas A_j and A_k where $j, k < i$.*

4. *The proof system must be consistent and complete.*

By Modus Ponens we mean the rule:

$$\frac{A \quad A \supset B}{B}$$

We write $A_1, \ldots, A_n \vdash_k B$ to mean that there is a sequence of $\leq k$ formulas each of which is one of the A_i's, is an axiom, or is inferred by modus ponens from earlier formulas such that B is the final formula of the proof.

Although it suffices to have modus ponens as the single inference rule to obtain a complete proof system, it is well-known that other modes of inference are also sound. The most notable example of this is the deduction rule which states that if a formula B has a proof from an additional, extra-logical hypothesis A (in symbols, $A \vdash B$) then there is a proof of $A \supset B$.

$$\frac{A \vdash B}{A \supset B} \qquad \text{Deduction Rule}$$

This paper establishes upper bounds on the proof speedups obtained by this rule on certain types of proofs and certain types of formulas. By a "speedup" of a proof, we mean the amount that proofs can be shortened with additional inference rules. In this paper, the *length* of a proof is the number of symbols in the proof.

If S and T are proof systems we say that S can linearly (respectively , quadratically) *simulate* T if, for any T-proof of k symbols, there is an S-proof of the same formula of $O(k)$ symbols (respectively, of $O(k^2)$ symbols). We say that T provides at most linear (respectively, quadratic) *speedup* over S if S can linearly (respectively, quadraticly) simulate T.

Counting length in terms of number of symbols, any two Frege systems simulate each other with at most polynomial increase in the length of the proofs if we change the set of connectives. See Reckhow [**?**] for a proof of this fact. If we only change the set of axiom schemata, again any two Frege

systems simulate each other with only linear increase in the length (number of symbols) of the proofs (see [**?**]). Therefore in this paper we fix the set of connectives, but not the set of axiom schemata. For an example of a complete set of axiom schemata see [**?**].

In section 2 we analyze the proof of the deduction theorem to show that Frege systems with the deduction rule provide at most quadratic speedup over the Frege systems. The second theorem proves that Frege systems linearly simulate tree-like Frege systems with the deduction rule.

The open question is whether Frege systems can do better than a quadratic simulation of the deduction Frege systems. The last two sections of this paper will consist on the analysis of some examples that seem to be the most likely to get an almost quadratic speedup when using the deduction rule. But in all our examples, we prove that the speed up is much less than quadratic.

Also there is an intermediate section (section 3) about ways to associate parenthesis on formulas, and how that leads into different ways of balancing trees.

Work on lengths of propositional proofs counting the number of symbols in a proof was done also by Cook-Reckhow [**?**, **?**] and Statman [**?**]. Also work on strengthenings of the deduction theorem but counting number of lines as a measure of length was done by Bonet-Buss [**?**, **?**, **?**].

2 The Deduction Theorem Counting the Number of Symbols

Let us make the following important comment before we prove any theorems in this section:

Note Say a fixed tautology B has $p_1, \ldots, p_n$ as propositional variables, and a proof of B has m symbols. Then if we substitute $p_1, \ldots, p_n$ by $A_1, \ldots, A_n$ respectively, then the resulting formula has a proof with at most $m(|A_1| + \ldots + |A_n|)$ symbols.

Theorem 1 *If $A \vdash B$ in n symbols, then $\vdash A \supset B$ in $O(n^2)$ symbols.*

Proof By the hypothesis, there is a proof of B from the assumption A that looks like:

$$\left\lceil \begin{array}{l} C_1 = A \\ C_2 \\ \vdots \\ C_m = B \end{array} \right.$$

To find a proof P of $A \supset B$ in the Frege system, we will transform the former proof into the sequence P':

$$\begin{array}{c} A \supset C_1 \\ A \supset C_2 \\ \vdots \\ A \supset C_m \end{array}$$

This is not really a Frege proof, but we can easily get a Frege proof by filling in the gaps the following way:

The first line is $A \supset A$. We need to introduce a proof of it at the beginning of P to justify that first line. This means an increase in length of $O(|A|)$ symbols. This is because if $p \supset p$ has a proof of a constant k number of symbols, then by the note $A \supset A$ has a proof in at most $k|A|$.

We need to fill in the rest of the lines to make up a proof. Let's justify $A \supset C_i$ for any i such that $2 \leq i \leq n$. We have two cases:

- C_i is an axiom. The proof of $A \supset C_i$ will consist of: axiom C_i, a proof of $C_i \supset (A \supset C_i)$ and a use of MP to get $A \supset C_i$. All this will have length $O(|A| + |C_i|)$.
- C_i was obtained by MP on C_j and C_k. Say $C_k = C_j \supset C_i$. Then in some former lines of P' we have $A \supset C_j$ and $A \supset C_k$. From these two former lines, we can justify $A \supset C_i$, and the number of symbols to do such justification is $O(|A| + |C_i| + |C_j|)$, or alternatively $O(|A| + |C_k|)$.

This way we get a proof P of $A \supset B$. In general each line $A \supset C_i$ can be justified with

$$d(|A| + |C_i| + |C_k|)$$

symbols, where d is a constant. Each formula in the proof of $A \vdash B$ will play the role of C_k only once, since each formula will be proven only once.

If we count the number of symbols of P, we get that it is at most

$$d(m \cdot |A| + \sum_{i=1}^{m} |C_i| + \sum_{i=1}^{m} |C_k|) \tag{1}$$

Also, all we know about A and m is that $|A| < n$ and $m < n$. So P has less than

$$d(n^2 + n + n) \tag{2}$$

symbols. Therefore $A \supset B$ has a proof in $O(n^2)$ symbols. $\square$

If we could bound m and $|A|$ so that $m \cdot |A| = O(n)$, then the above argument shows that we can obtain a proof of $A \supset B$ with $O(n)$ symbols. But it is possible to have a proof where both $|A|$ and m are $O(n)$. In fact the examples we are going to be working with have big $|A|$'s and m's. Before we look into these examples, let us show that Frege systems linearly simulate tree-like Frege systems with the deduction rule.

Definition 2 *We say a proof P is tree-like if each line in P is used only once in the proof. By used in a proof we mean to be a hypothesis of a MP inference. Also, if $A \vdash B$, then A can occur more than once in the proof.*

Definition 3 *Given $A \vdash B$, we say A is used in a linear way if all the lines $A_1, \ldots, A_s$ in the proof that depend on A are obtained the following way: there are lines $\varphi_1, \ldots, \varphi_s$ in the proof that don't depend on A (i.e. they can be proved without any hypothesis) such that $\forall i, 1 \leq i \leq s$, A_i is obtained by MP on φ_i and A_{i-1}, A_1 is obtained by MP on φ_1 and A, and $A_s = B$. Pictorically, $A \vdash B$ looks like*

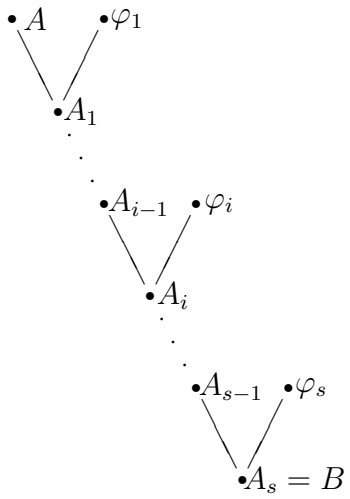

Figure 1

where the φ_i's have their proofs possibly non tree-like.

Lemma 2 *If $A \vdash B$ is tree-like and A occurs only once in the proof, then also A is used in a linear way.*

However, the opposite is not true, since the formulas $\varphi_1, \ldots, \varphi_s$ could have been obtained in a non tree-like manner. The next theorem is due to S. Buss.

Theorem 3 *Suppose that $A \vdash B$ in n symbols, with A used in a linear way. Then $\vdash A \supset B$ in $O(n)$ symbols.*

Proof Say P is the proof of B from the hypothesis A in n symbols. Say $A_1, \ldots, A_s$ are the lines in the proof that depend on the hypothesis A. Also there are lines $\varphi_1, \ldots, \varphi_s$ such that each A_i is obtained by MP from φ_i and A_{i-1}. Note that $A_s = B$, since B should depend on A, otherwise B would be provable without assuming A.

Let us create the following sequence P':

$$\begin{array}{l}
\varphi_1 \supset (A \supset A_1) \\
\varphi_2 \supset (A_1 \supset A_2) \\
\vdots \\
\varphi_s \supset (A_{s-1} \supset A_s) \\
\\
A \supset A_1 \\
A_1 \supset A_2 \\
\vdots \\
A_{s/2-1} \supset A_{s/2} \\
A_{s/2} \supset A_{(s/2)_+1} \\
\vdots \\
A_{s-1} \supset A_s \\
\\
A_{(s/2)-1} \supset A_{(s/2)+1} \\
A_{(s/2)-2} \supset A_{(s/2)+2} \\
A_{(s/2)-3} \supset A_{(s/2)+3} \\
\vdots \\
A_1 \supset A_{s-1} \\
A \supset A_s
\end{array}$$

The first s lines of the sequence above have less than $O(n)$ symbols because each formula A_i appears only twice, and $|\varphi_i|$ is $O(|A_{i-1}| + |A_i|)$. The second set of s lines has again less than $2 \cdot n$ symbols because each formula of the proof P appears at most twice. The last $s/2$ lines of the sequence above have less than n symbols because each formula appears only once. Therefore, the sequence above has at most $5 \cdot n$ symbols.

From the sequence P' we want to create a proof P_1 of $A \supset B$ in $O(n)$ symbols. To do that we need to justify each line, i.e., to fill in the blanks in P'.

In the first group of s lines each line $\varphi_i \supset (A_{i-1} \supset A_i)$ is justified by adding to the proof $O(|\varphi_i| + |A_{i-1}| + |A_i|)$ symbols. Since each formula A_i shows in the first lines of P' at most twice, and $|\varphi_i|$ is $O(|A_{i-1}| + |A_i|)$, the first s lines can be justified in $O(n)$ symbols. The reason we worry about $|\varphi_i|$ is because some φ_i's could be identical, and they wouldn't be repeated in the original proof as they would in P'.

The second set of s lines can be justified very easily. P contains a subproof that doesn't depend on A and proves all the φ_i's. Insert this subproof between the first and second set of s lines. This subproof has $< n$ symbols since it is just part of P. Now with s uses of MP (using the first s lines of P'), we can get the second set of s lines. The total number of symbols added is $O(n)$.

Now let us explain how to justify the last $s/2$ lines. We get each $A_{(s/2)-i} \supset A_{(s/2)+i}$ from the former lines, assuming we have justified lines $A_{(s/2)-i} \supset A_{(s/2)-(i-1)}$, $A_{(s/2)-(i-1)} \supset A_{(s/2)+(i-1)}$, and $A_{(s/2)+(i-1)} \supset A_{(s/2)+i}$. To obtain $A_{(s/2)-i} \supset A_{(s/2)+i}$ we add $O(|A_{(s/2)-i}| + |A_{(s/2)-i+1}| + |A_{(s/2)+i-1}| + |A_{(s/2)+i}|)$ symbols. Note that $A_{(s/2)-(i-1)}$ and $A_{(s/2)+(i-1)}$ were used in the line before, but they won't be used anymore in the sequence. Also $A_{(s/2)-i}$ and $A_{(s/2)+i}$ were not used before, but they will be used to justify the next line and then not used anymore. So each line A_i from P is used a constant number of times to justify the last $s/2$ lines. Therefore the number of symbols added to justify the last $s/2$ lines is $O(n)$ also.

Therefore the proof P_1 obtained by filling in the blanks of P' as explained above has $O(n)$ symbols. □

If we analyze the former proof, and compare it with what we did in theorem **??**, we will see that the reason why we don't get the quadratic increase is because we don't have to put $A \supset$ in front of each line. In fact, for all A_i, we put $A_i \supset$ in front of a line only a constant number of times in the sequence.

Corollary 4 *Suppose that $A \vdash B$ in n symbols, A occurs only once and the proof is tree-like. Then $\vdash A \supset B$ in $O(n)$ symbols.*

Theorem 5 *Suppose that $A \vdash B$ in n symbols, and the proof is tree-like. Then $\vdash A \supset B$ in $O(n)$ symbols.*

Proof We prove that $\vdash A \supset B$ in $c(3n - |A| - |B|)$ symbols for some constant c, by induction on the number of occurences of A in the tree-like proof. Suppose the theorem is true for all proofs where A occurs less than l times. We are going to prove it for $l \geq 2$ (if $l = 1$ it's true by the former corollary).

Say $A \vdash B$ has l occurences of A, and it looks as figure 1, where now the φ_i's have tree-like proofs, and some of them depend on A. Say A_i is such

that A_{i-1} and φ_i depend on A, but for all $j > i$ φ_j doesn't depend on A (this always happens since $l \geq 2$). Also say the proof of $A \vdash A_{i-1}$ has m_1 symbols, the proof of $A \vdash \varphi_i$ has m_2 symbols, and the proof of $A_i \vdash B$ (the rest) has m_3 symbols. So $m_1 + m_2 + m_3 = n$. In the proof of $A_i \vdash B$, A_i was used in a linear way, since the φ_j's for $j > i$ don't depend on any hypothesis. So by the theorem **??**, we can obtain a proof of $\vdash A_i \supset B$ in $O(m_3)$ symbols, say in $d \cdot m_3$ symbols. Also by the induction hypothesis, there are proofs of $A \supset A_{i-1}$ and $A \supset \varphi_i$ of length $c(3m_1 - |A| - |A_{i-1}|)$ and $c(3m_2 - |A| - |\varphi_i|)$ respectively, since A occurs less than l times in those subproofs. We can obtain a proof of $A \supset B$ the following way:

$$\left.\begin{array}{c}\vdots \\ A \supset A_{i-1}\end{array}\right\} \quad c(3m_1 - |A| - |A_{i-1}|)$$

$$\left.\begin{array}{c}\vdots \\ A \supset \varphi_i\end{array}\right\} \quad c(3m_2 - |A| - |\varphi_i|)$$

$$\left.\begin{array}{c}\vdots \\ A_i \supset B\end{array}\right\} \quad dm_3$$

$$\left.\begin{array}{c}A_{i-1} \wedge \varphi_i \supset A_i \\ A \supset A_i \\ A \supset B\end{array}\right\} \quad d_1(|A_{i-1}| + |\varphi_i| + |A_i| + |A| + |B|)$$

Note that if $A_i = A_s = B$, then we don't have to do the work in the third section.

Adding up all the work we get a proof with at most

$$c(3m_1 + 3m_2) + (d_1|A| - 2c|A|) + (d_1|A_{i-1}| - c|A_{i-1}|) + (d_1|\varphi_i| - c|\varphi_i|) + (dm_3 + d_1|B| + d_1|A_i|)$$

number of symbols. Since $dm_3 + d_1|A_i| + d_1|B| \leq m_3(d + d_1)$, taking $c \geq d + d_1$, we get that the number of symbols in the proof is

$$\begin{array}{rl} \leq & c(3m_1 + 3m_2) - c|A| + cm_3 \\ \leq & c(3m_1 + 3m_2 + 3m_3 - 2m_3 - |A|) \\ \leq & c(3n - |B| - |A|). \end{array}$$

So the result follows. □

3 Balanced and Pseudobalanced Trees and Formulas

Definition 4 *We say a tree is binary if each node has degree at most two. We say a binary tree is complete if each node has degree either zero or two, and all the leaves (i.e. nodes of degree zero) are at the same depth.*

Definition 5 *A tree T is balanced if for every subtree T' of T of n leaves, the left immediate subtree of T' has $\lceil (n-1)/2 \rceil$ leaves, and the right immediate subtree of T' has $\lfloor (n-1)/2 \rfloor$ leaves.*

Definition 6 *A tree T is pseudobalanced if for every subtree T' of T, the left immediate subtree of T' is a complete binary tree, and the right immediate subtree of T' has at most as many nodes as the left immediate subtree.*

Fact: A complete binary tree is balanced and pseudobalanced.

Parenthesis on formulas can be associated in several different ways. In this paper, we are going to do it in a pseudobalanced way, following the tree model. In fact we can view a formula as a tree, and depending on how the parenthesis are associated, the tree that it represents can be more or less balanced. But before we look at ways to parenthesise a formula, let us see how formulas are represented by trees. Given a formula F,

i) if F is atomic, $F = p$, then the tree has one node and zero edges. The node is labeled as p.

ii) if F is $(A \wedge B)$, $(A \supset B)$ or $(A \vee B)$, then F represents a tree that has a root labeled $\wedge$, $\supset$ or $\vee$, and A represents the left immediate subtree, and B the right immediate subtree. If F is $\neg(A)$, then the root of the tree is labeled $\neg$, and A represents the left immediate subtree of the tree rooted at $\neg$. Such a tree won't have a right immediate subtree.

Definition 7 *A formula A is binary, if it only contains connectives $\wedge$, $\vee$ and $\supset$.*

Definition 8 *The depth of a formula is the height of the tree that represents it.*

Definition 9 *A binary formula is completely balanced if the tree that represents is a complete binary tree. Thus, a completely balanced binary formula has 2^n atomic formulas and $2^n - 1$ connectives, where n can be any natural number. A formula is balanced, if the tree that represents it is balanced. A formula is pseudobalanced, if the tree that represents it is pseudobalanced.*

The definitions of balanced and pseudobalanced formula make sense for binary formulas only, since the presence of $\neg$ makes the formula harder to balance. Although, one way to balance non-binary formulas would be to push $\neg$'s down to the leaves, and then pseudobalance the formula.

Let us now give some examples of balanced and pseudobalanced:

Example 1: A balanced formula like

$$[((A_1 \wedge A_2) \wedge A_3) \wedge ((A_4 \wedge A_5) \wedge A_6)] \wedge [((A_7 \wedge A_8) \wedge A_9) \wedge (A_{10} \wedge A_{11})]$$

produces a highly balanced tree:

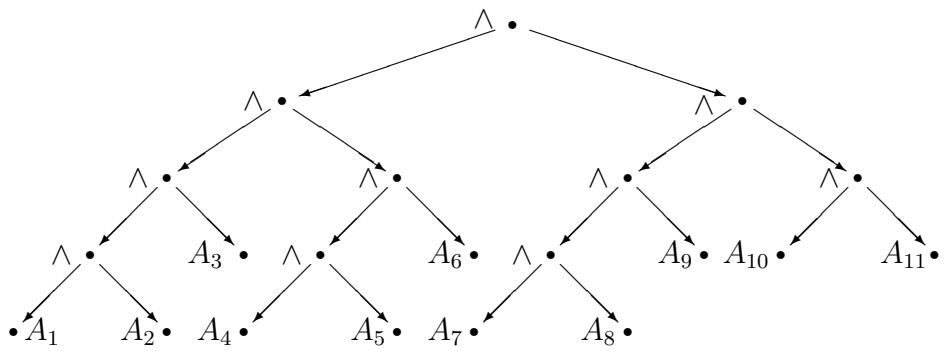

Figure 2

Example 2: A pseudobalanced formula like

$$[((A_1 \wedge A_2) \wedge (A_3 \wedge A_4)) \wedge ((A_5 \wedge A_6) \wedge (A_7 \wedge A_8))] \wedge ((A_9 \wedge A_{10}) \wedge A_{11})$$

produces the following tree:

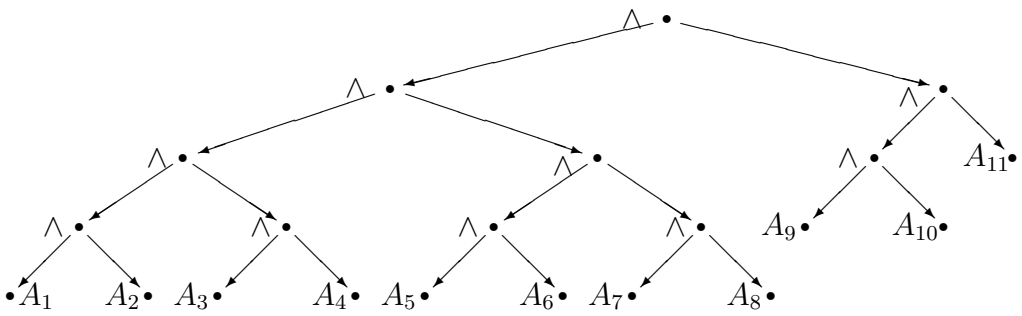

Figure 3

Notice that the depth of the tree is actually the same in the balanced tree.

Now let us prove some facts about what it takes to restore the pseudobalanced property on trees and formulas. Given two pseudobalanced formulas, we will study how many symbols it takes to prove that the conjunction of them implies a new pseudobalanced formula. And if we take two pseudobalanced trees and make a new tree by making each one be an immediate subtree of the root, we will see how can we restore the pseudobalanced property in the new tree. Before we prove these facts, let us define the notion of operations on trees, and what it means to pseudobalance a tree:

Definition 10 *There are two kinds of tree operations:*

1. *Given a node X with left child Y and right child Z, then the operation of switching T_Y and T_Z is a permutation operation.*

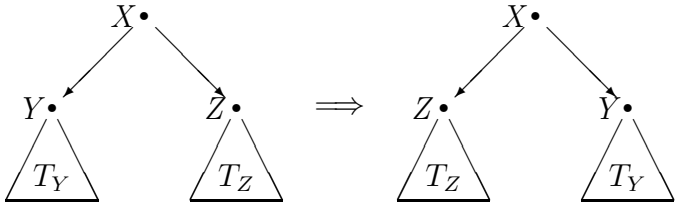

Figure 4

2. *The second kind is called a rotation operation. The notion is best explained by the figure below:*

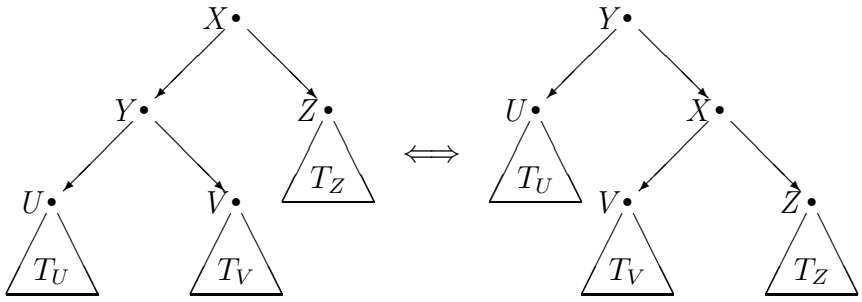

Figure 5

When we go from the picture on the left to the one on the right, we say we perform a right rotation on Y. When we go from the picture on the right to the one on the left, we say we perform a left rotation on X.

The second type of operation is a well-known one. For more information see [**?**]. Since we can represent formulas as binary tree, let us see the effect on formulas and on the association of parenthesis that these two operations have. The permutation operation corresponds to:

$$(A \wedge B) \Longrightarrow (B \wedge A)$$

The rotation operation corresponds to:

$$((A \wedge B) \wedge C) \Longrightarrow (A \wedge (B \wedge C))$$

and

$$(A \wedge (B \wedge C)) \Longrightarrow ((A \wedge B) \wedge C)$$

Definition 11 *Let T be a binary tree. To pseudobalance T means to obtain a pseudobalance tree T' by doing a succession of tree operations on T. Note that the leaves might be permuted doing the tree operations.*

Theorem 6 *Let T_1 and T_2 be two pseudobalanced binary trees, and let T be the binary tree such that T_1 is the left immediate subtree, and T_2 is the right immediate subtree of the root of T. Let n be the number of leaves in T. Then T can be pseudobalanced with $O(n)$ tree operations.*

Proof by induction on the number of leaves. Suppose the theorem holds for all numbers $< n$. We will prove it for n. Say T_1 has n_1 leaves, and T_2 has n_2 leaves ($n = n_1 + n_2$). Also say $n_1 = 2^r + a$ and $n_2 = 2^s + b$, where $1 \leq a \leq 2^r$ and $1 \leq b \leq 2^s$. Assume w.l.o.g. that $n_1 \geq n_2$. We will label the root of T as X, the root of T_1 as X_1, the root of T_2 as X_2. Also, the roots of the left and right immediate subtrees of T_1 and T_2 are X_{i_L} and X_{i_R} for $i = 1, 2$. The tree T looks as in the figure below.

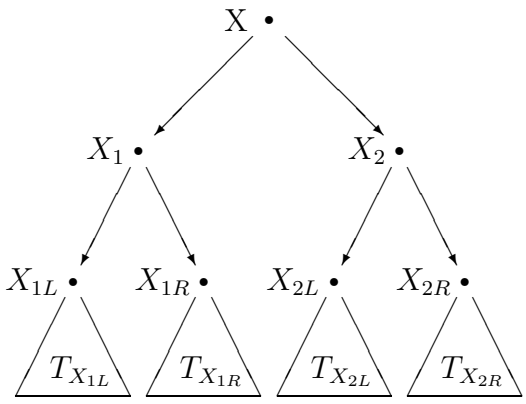

Figure 6

$T_{X_{1_L}}$ and $T_{X_{1_R}}$ have 2^r and a leaves respectively, and $T_{X_{2_L}}$ and $T_{X_{2_R}}$ have 2^s and b leaves respectively.

Case 1: $r = s$. We want to interchange the trees $T_{X_{1_R}}$ and $T_{X_{2_L}}$. For that we have to do the following sequence of 5 operations: right rotation on X_1, left rotation on X_2, permutation of $T_{X_{1_R}}$ and $T_{X_{2_L}}$, right rotation on X, left rotation on X.

Now the left immediate subtree of X is a complete binary tree since $r = s$, and we need to make the right immediate subtree of X a pseudobalanced tree. For that we will use the induction hypothesis on $a + b$. With say $c(a + b)$ operations we can pseudobalance T_{X_2}. At this point T is pseudobalanced, and we have used $c(a + b) + 5$ operations. $c(a + b) + 5 \leq c \cdot n$ for $c \geq 2$.

Case 2: $r > s$. Doing a right rotation on X_1 (see figure 12) we obtain the tree:

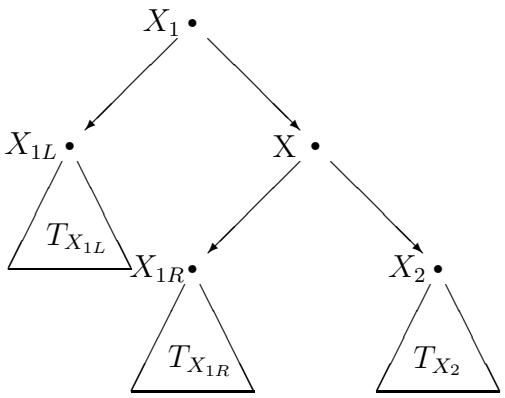

Figure 7

We want to pseudobalance the new subtree rooted at X of $a + b + 2^s$ leafs. By the induction hypothesis, we can do that with $c(a + b + 2^s)$ operations, obtaining a new tree rooted at X. If $a+b+2^s \leq 2^r$, then we are finished at this point, since the whole tree is then pseudobalanced. But if $a + b + 2^s > 2^r$, we are not finished. Since $b \leq 2^s$ and $s < r$, then $b + 2^s \leq 2 \cdot 2^s < 2^r$. Also, $a \leq 2^r$, so $a + b + 2^s < 2^{r+1}$. So $a + b + 2^s = 2^r + c$ for $c < 2^r$. So if $a + b + 2^s > 2^r$, the tree looks like:

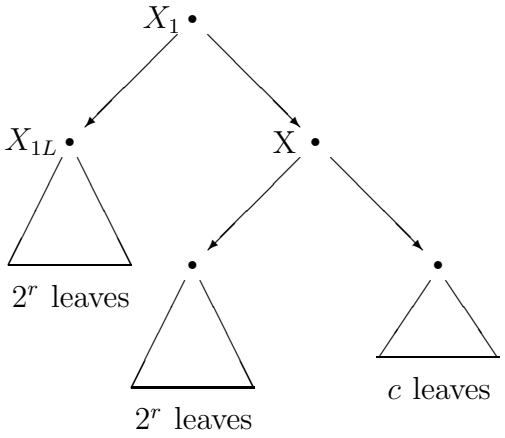

Figure 8

At this point, doing a left rotation on X, we obtain a pseudobalanced

tree. We have done at most $c(a+b+2^s)+2$ operations. It is clear that $c(a+b+2^s)+2 \leq c \cdot n$ for $c \geq 1$.

The result follows for $c = 2$. $\Box$.

The former theorem can be improved to theorem **??**. In theorem **??** we don't count number of operations, but number of symbols.

Theorem 7 *Let* $\bigwedge_{i=1}^{t} A_i$ *and* $\bigwedge_{i=t+1}^{n} A_i$ *be pseudobalanced formulas. Then there is a permutation* $i \to j_i$ *(for* $i = 1, \ldots, n$*) and a pseudobalanced formula* $\bigwedge_{i=1}^{n} A_{j_i}$ *such that the formula*

$$\bigwedge_{i=1}^{t} A_i \wedge \bigwedge_{i=t+1}^{n} A_i \supset \bigwedge_{i=1}^{n} A_{j_i}$$

has a proof in $O(n)$ *symbols.*

Proof by induction on n. Suppose the theorem holds for all numbers $< n$. Say $t = 2^r + a$, $n - t = m$, and $m = 2^s + b$, where $0 \leq a \leq 2^r$, $0 \leq b \leq 2^s$, and say $r \geq s$.

Case 1: $r = s$. The formula

$$\bigwedge_{i=1}^{t} A_i \wedge \bigwedge_{i=t+1}^{n} A_i \supset [\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=t+1}^{t+2^r} A_i] \wedge [\bigwedge_{i=2^r+1}^{t} A_i \wedge \bigwedge_{i=t+2^r+1}^{t+m} A_i] \tag{3}$$

is provable in $O(n)$ symbols. We can apply the induction hypothesis to $a + b \leq n$, and get

$$\bigwedge_{i=2^r+1}^{t} A_i \wedge \bigwedge_{i=t+2^r+1}^{t+m} A_i \supset \bigwedge_{i=1}^{a+b} A_{s_i} \tag{4}$$

in $O(a+b)$ symbols, say $c(a+b)$ symbols, where $i \to s_i$ is a permutation for $2^r + 1 \leq i \leq t$ or $t + 2^r + 1 \leq i \leq t + m$. Also

$$[\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=t+1}^{t+2^r} A_i] \wedge [\bigwedge_{i=2^r+1}^{t} A_i \wedge \bigwedge_{i=t+2^r+1}^{t+m} A_i] \supset [\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=t+1}^{t+2^r} A_i] \wedge \bigwedge_{i=1}^{a+b} A_{s_i} \tag{5}$$

is provable with $O(n)$ extra symbols from formula (**??**). Finally we get

$$[\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=2^r+1}^{t} A_i] \wedge [\bigwedge_{i=t+1}^{t+2^r} A_i \wedge \bigwedge_{i=t+2^r+1}^{t+m} A_i] \supset [\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=t+1}^{t+2^r} A_i] \wedge \bigwedge_{i=1}^{a+b} A_{s_i}$$

with extra $O(n)$ symbols from formulas (**??**) and (**??**). This last formula is what we wanted to show. The total number of symbols we have used is: $c(a+b) + d \cdot n$ for some constant d. We are going to show that if we pick $c \geq 2 \cdot d$, then $c(a+b) + d \cdot n \leq c \cdot n$, and the result follows for this case. If $d \leq c/2$, then

$$\begin{aligned} c(a+b) + d \cdot (a+b+2^r \cdot 2) &\leq c(a+b) + d \cdot (2^r \cdot 2 + 2^r \cdot 2) \\ &\leq c(a+b) + c/2 \cdot (2^r \cdot 2 + 2^r \cdot 2) \\ &\leq c \cdot n \end{aligned}$$

Case 2: $s < r$. By the induction hypothesis applied to $a + b + 2^s$, we get a proof of

$$\bigwedge_{i=2^r+1}^{t} A_i \wedge \bigwedge_{t+1}^{t+m} A_i \supset \bigwedge_{i=1}^{a+m} A_{j_i} \tag{6}$$

in $O(a+m)$ symbols, where $i \to j_i$ is a permutation for $2^r < i \leq t+m$. From formula (**??**) we get with $O(n)$ extra symbols:

$$\bigwedge_{i=1}^{2^r} A_i \wedge [\bigwedge_{i=2^r+1}^{t} A_i \wedge \bigwedge_{t+1}^{t+m} A_i] \supset \bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=1}^{a+m} A_{j_i} \tag{7}$$

Since we can prove in $O(n)$ symbols

$$[\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=2^r+1}^{t} A_i] \wedge \bigwedge_{t+1}^{t+m} A_i \supset \bigwedge_{i=1}^{2^r} A_i \wedge [\bigwedge_{i=2^r+1}^{t} A_i \wedge \bigwedge_{t+1}^{t+m} A_i], \tag{8}$$

then from (**??**) and (**??**) with $O(n)$ extra symbols we prove

$$\bigwedge_{i=1}^{t} A_i \wedge \bigwedge_{i=t+1}^{t+m} A_i \supset \bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=1}^{a+m} A_{j_i} \tag{9}$$

If $a + m \leq 2^r$, then we are finished at this point, since $\bigwedge^{2^r}( ) \wedge \bigwedge^{a+m}( )$ is then pseudobalanced. But if $a + m > 2^r$, we are not finished. Since

$b < 2^s$ and $s < r$, then $m = b + 2^s < 2 \cdot 2^s < 2^r$. i.e., $m < 2^r$. Also, $a < 2^r$, so $a + m < 2^{r+1}$. So $a + m = 2^r + e$ for $e < 2^r$. So formula (**??**) is actually the formula

$$\bigwedge_{i=1}^{t} A_i \wedge \bigwedge_{i=t+1}^{t+m} A_i \supset \bigwedge_{i=1}^{2^r} A_i \wedge [\bigwedge_{i=1}^{2^r} A_{j_i} \wedge \bigwedge_{i=2^r+1}^{e} A_{j_i}] \tag{10}$$

where $\bigwedge_{i=2^r+1}^{c} A_{j_i}$ is pseudobalanced. With $O(n)$ symbols we get from formula (**??**)

$$\bigwedge_{i=1}^{t} A_i \wedge \bigwedge_{i=t+1}^{t+m} A_i \supset [\bigwedge_{i=1}^{2^r} A_i \wedge \bigwedge_{i=1}^{2^r} A_{j_i}] \wedge \bigwedge_{i=2^r+1}^{e} A_{j_i} \tag{11}$$

which is what we wanted to show.

We have used a total of $c(a+m)+d' \cdot n$ symbols, where d' is a constant. We need to show that

$$c(a + m) + d' \cdot n \leq c \cdot n.$$

Taking $c \geq 3d'$, since $a + m < 2^{r+1}$,

$$\begin{aligned} d' \cdot n + c(a + m) &\leq d'(a + m + 2^r) + c(a + m) \\ &\leq d' \cdot 3 \cdot 2^r + c(a + m) \\ &\leq c \cdot 2^r + c(a + m) = c \cdot n \end{aligned}$$

So the result follows taking $c = 3 \cdot \max(d, d')$. □

We can prove a variant of theorem **??** which states how many symbols are required to prove that an arbitrary conjunction implies a pseudobalanced conjunction.

Theorem 8 *Let* $\bigwedge_{i=1}^{n} A_i$ *be a non-pseudobalanced formula of depth* d*. Then, there is a permutation* $i \to j_i$ *(for* $i = 1, \ldots, n$*) and a pseudobalanced formula* $\bigwedge_{i=1}^{n} A_{j_i}$ *such that*

$$\bigwedge_{i=1}^{n} A_i \supset \bigwedge_{i=1}^{n} A_{j_i}$$

has a proof in $O(n \cdot d)$ *symbols.*

Proof by induction on n. Suppose the fact is true for all numbers $< n$.

Say $\bigwedge\!\!\!\bigwedge_{i=1}^{n} A_i = \bigwedge\!\!\!\bigwedge_{i=1}^{t} A_i \wedge \bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_i$, and the depth of $\bigwedge\!\!\!\bigwedge_{i=1}^{t} A_i$ is n_1, the depth of $\bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_i$ is n_2 and w.l.o.g., $n_1 \geq n_2$. Then the depth of $\bigwedge\!\!\!\bigwedge_{i=1}^{n} A_i$ is $n_1 + 1$. Now, by the induction hypothesis

$$\bigwedge\!\!\!\bigwedge_{i=1}^{t} A_i \supset \bigwedge\!\!\!\bigwedge_{i=1}^{t} A_{s_i}$$

and

$$\bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_i \supset \bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_{s_i}$$

can be proved with say ctn_1 and $c(n-t)n_2$ symbols respectively, for the same constant c. The consequents of those formulas are a permutation of the antecedents pseudobalanced. Also with say $d_1 \cdot n$ symbols, we can get

$$\bigwedge\!\!\!\bigwedge_{i=1}^{t} A_i \wedge \bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_i \supset \bigwedge\!\!\!\bigwedge_{i=1}^{t} A_{s_i} \wedge \bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_{s_i}.$$

By theorem **??** in say $d_2 \cdot n$ symbols we can show

$$\bigwedge\!\!\!\bigwedge_{i=1}^{t} A_{s_i} \wedge \bigwedge\!\!\!\bigwedge_{i=t+1}^{n} A_{s_i} \supset \bigwedge\!\!\!\bigwedge_{i=1}^{n} A_{j_i}.$$

i.e. we obtain a pseudobalanced formula from the conjunction of two pseudobalanced ones. Finally, with say $d_3 \cdot n$ symbols more we prove

$$\bigwedge\!\!\!\bigwedge_{i=1}^{n} A_i \supset \bigwedge\!\!\!\bigwedge_{i=1}^{n} A_{j_i}$$

The total number of symbols used is $ctn_1 + c(n-t)n_2 + (d_1 + d_2 + d_3)n$. If we take $c \geq d_1 + d_2 + d_3$, then

$$\begin{aligned} ctn_1 + c(n-t)n_2 + (d_1 + d_2 + d_3)n &\leq ctn_1 + c(n-t)n_2 + cn \\ &\leq ctn_1 + c(n-t)n_1 + cn \\ &\leq cnn_1 + cn = cn(n_1 + 1) \end{aligned}$$

The result follows. □

4 Number of Symbols in Proofs of Permutation Formulas

In this last two sections we are going to talk about two types of propositional formulas, that seem most likely to produce an almost quadratic speed up when using the deduction rule. The first formula to consider is

$$\bigwedge_{i=1}^{n} p_i \supset \bigwedge_{i=1}^{n} p_{j_i} \tag{12}$$

where $i \to j_i$ is any permutation for i such that $1 \leq i \leq n$, and both antecedent and consequent are pseudobalanced. Formula **??** means that a conjunction of atomic formulas implies any permutation of the atoms. We will study the lengths of proofs (counting number of symbols) of such formulas with and without the deduction rule.

Let us first give a sketch of theorem due to Buss which implies that any proof of formula (**??**) requires $\Omega(n \log n)$ symbols. If A is a tautology and B is a subformula, then we write $A(B/\top)$ and $A(B/\bot)$ to denote the formulas obtained by replacing every occurence of B in A by $\top$ (a fixed tautology) and by $\bot$ (i.e., $\neg\top$), respectively. The subformula B is *needed* in A iff at least one of $A(B/\top)$ or $A(B/\bot)$ is not a tautology. Now suppose A is a tautology with proof P and let X be the set of formulas which are needed in A. Then we claim that the number of symbols in P has the lower bound $\Omega(\sum_{B\in X} |B|)$. To prove this, consider any axiom φ in P; φ is of course an instance of an axiom schema ψ: we say that a subformula B of φ is *affected* by the axiom φ iff some occurence of B in φ has principle connective corresponding to a connective from the schema ψ. It is easy to see that any formula B needed in A must either be affected by some axiom in the proof P or be used as the (second) hypothesis of a modus ponens inference in P; since otherwise every occurence of B in P could be replaced by $\top$ or $\bot$ to yield proofs of $A(B/\top)$ and $A(B/\bot)$, respectively. Since an axiom can affect only a bounded number of formulas, the lower bound on the size of P follows.

For a special case of this lower bound, suppose that A is a tautology, that no non-atomic subformula occurs twice in A and that every non-atomic subformula of A is needed in A. Then any proof P of A requires $\Omega(s)$ symbols where

$$s = \sum \{ \mathit{depth}(q) : q \text{ is an } \mathit{occurence} \text{ of a variable in } A \} .$$

As a special case, Buss's lower bound shows that, in general, formula (**??**) will require $\Omega(n \log n)$ symbols. An important observation is that the same lower bound applies (by the same argument as above) to proofs of (**??**) with the deduction rule.

With the deduction rule we can easily produce an optimal length proof of (**??**), with $O(n \log n)$ symbols, the following way: first assume $\bigwedge_{i=1}^{n} A_i$. For simplicity, we will assume that n is a power of 2. We obtain

$$\bigwedge_{i=1}^{n/2} A_i \quad \text{and} \quad \bigwedge_{i=(n/2)+1}^{n} A_i.$$

Then we get

$$\bigwedge_{i=1}^{n/4} A_i, \quad \bigwedge_{i=(n/4)+1}^{n/2} A_i, \quad \bigwedge_{(n/2)+1}^{3n/4} A_i, \quad \text{and} \quad \bigwedge_{i=(3n/4)+1}^{n} A_i$$

etc., until finally we obtain

$$A_1, \quad A_2, \quad \ldots, \quad A_n.$$

This process takes $O(n \log n)$ symbols and $O(n)$ lines. We reverse the process to obtain $\bigwedge_{i=1}^{n} A_{j_i}$ in $O(n \log n)$ symbols and $O(n)$ lines more. With the deduction rule we obtain (**??**) with $O(n \log n)$ symbols and $O(n)$ lines.

If we try to prove the same formula in the Frege system, using the methods of theorem **??** we would obtain a proof of $O(n^2)$ symbols, since the proof with the deduction rule has n lines, and $\bigwedge_{i=1}^{n} A_i$ has size n (see equations **??** and **??**). But, can we give a Frege proof of (**??**) with less than $O(n^2)$ symbols? The answer is yes. We are going to produce a proof of (**??**) of $O(n \log^2 n)$ symbols without the deduction rule. So we obtain a $O(n/\log^2 n)$ speedup over theorem **??**. It is still open whether there is a Frege-proof of (**??**) with $O(n \log n)$ symbols. Only in some cases we were able to obtain proofs of permutation formulas in $O(n \log n)$ without the deduction rule. Let us see one example:

Lemma 9 *For every m, the formula*

$$\bigwedge_{i=1}^{2^m} q_i \supset \bigwedge \{q_1, q_{(2^m/2)+1}, q_2, q_{(2^m/2)+2}, \ldots, q_{2^m/2}, q_{2^m}\}$$

where antecedent and consequent are completely balanced, has a proof in $O(n \log n)$ *symbols, where* $n = 2^m$.

Proof by induction on m. Suppose the result is true for all numbers $< m$.

By the induction hypothesis, the formulas

$$\bigwedge_{i=1}^{n/4} q_i \wedge \bigwedge_{i=(n/2)+1}^{3n/4} q_i \supset \bigwedge\{q_1, q_{(n/2)+1}, q_2, q_{(n/2)+2}, \ldots, q_{n/4}, q_{3n/4}\} \tag{13}$$

and

$$\bigwedge_{(n/4)+1}^{n/2} q_i \wedge \bigwedge_{(3n/4)+1}^{n} q_i \supset \bigwedge\{q_{(n/4)+1}, q_{(3n/4)+1}, q_{(n/4)+2}, q_{(3n/4)+2}, \ldots, q_{n/2}, q_n\} \tag{14}$$

have proofs of $O((n/2)\log(n/2))$ symbols.

Say that $E = \bigwedge\{q_1, q_{(n/2)+1}, q_2, q_{(n/2)+2}, \ldots, q_{n/4}, q_{3n/4}\}$ and $F = \bigwedge\{q_{(n/4)+1}, q_{(3n/4)+1}, q_{(n/4)+2}, q_{(3n/4)+2}, \ldots, q_{n/2}, q_n\}$. From (**??**) and (**??**) we can obtain

$$[\bigwedge_{i=1}^{n/4} q_i \wedge \bigwedge_{i=(n/2)+1}^{3n/4} q_i] \wedge [\bigwedge_{(n/4)+1}^{n/2} q_i \wedge \bigwedge_{(3n/4)+1}^{n} q_i] \supset E \wedge F \tag{15}$$

with $O(n)$ extra symbols. From (**??**) we can prove

$$[\bigwedge_{i=1}^{n/4} q_i \wedge \bigwedge_{(n/4)+1}^{n/2} q_i] \wedge [\bigwedge_{i=(n/2)+1}^{3n/4} q_i \wedge \bigwedge_{(3n/4)+1}^{n} q_i] \supset E \wedge F$$

in $O(n)$ extra symbols, which is what we wanted to show.

So we have used a total of say $2c(n/2)\log(n/2) + dn$ symbols. Since $2c(n/2)\log(n/2) + dn = c \cdot n \cdot \log n - c \cdot n + d \cdot n$, the result follows taking $c \geq d$. $\square$

In general, for any possible permutation, there is a proof in $O(n \log^2 n)$ symbols. But before we prove this, let us prove the following lemmas:

Lemma 10 *Let* $\bigwedge_{i=1}^{m} q_i$ *be a pseudobalanced formula such that* $\bigwedge_{i=1}^{m} q_i = \bigwedge_{i=1}^{2^r} q_i \wedge \bigwedge_{i=2^r+1}^{m} q_i$. *Let* n *be the smallest power of* 2 *bigger than* m. *Let* $\bigwedge_{i=1}^{n} A_i$ *be a*

completely balanced formula where each A_i *is either* $\top$ *(where* $\top$ *is any fixed tautology) if* $i > m$ *or* q_i *if* $i \leq m$*. Then we can prove the formulas*

$$\bigwedge_{i=1}^{m} q_i \supset \bigwedge_{i=1}^{n} A_i \quad \textit{and} \quad \bigwedge_{i=1}^{n} A_i \supset \bigwedge_{i=1}^{m} q_i$$

in $O(n \log n)$ *symbols.*

Proof by induction on n. The proof is left to the reader.

Definition 12 *Let* A *be a binary formula, and let* T *be the tree that represents* A*. An* <u>*extract*</u> *of* A *is a formula represented by a tree* T' *obtained by the following process:*

1. *Removing from* T *any subset of the leaves of* T*.*
2. *If a node* x *labeled* $\wedge$*,* $\vee$ *or* $\supset$ *has only one child, we remove* x *and connect the child to the ancestor of* x*. Also we remove the edge from the ancestor of* x *to* x*.*
3. *If a non leaf node has no children, we remove it as well as the edge going to it.*

Operations 2 and 3 are to be performed iteratively as long as possible.

So an extract of a formula A, is a formula where we pulled out some atomic subformulas and extra connectives and parenthesis, but keeping the structure of A on what is left over.

Lemma 11 *Let* $\bigwedge_{i=1}^{n} q_i$ *be a completely balanced formula, and for* $m \leq n$*,* $\bigwedge_{i=1}^{m} A_i$ *is an extract of* $\bigwedge_{i=1}^{n} q_i$*, possibly unbalanced formed by removing some of the* q_i *'s from* $\bigwedge_{i=1}^{n} q_i$*. Then,*

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{m} A_i$$

has a proof in $O(n \log n)$ *symbols.*

Proof by induction on n. Suppose the fact is true for all powers of two $< n$. By the induction hypothesis,

$$\bigwedge_{i=1}^{n/2} q_i \supset \bigwedge_{i=1}^{t} A_i$$

and

$$\bigwedge_{i=(n/2)+1}^{n} q_i \supset \bigwedge_{i=t+1}^{m} A_i$$

have proofs of say $c(n/2)\log(n/2)$ symbols where t is the number of q_i's that we want to keep from the first half of the conjunction. With extra $O(n)$ symbols we get

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{t} A_i \wedge \bigwedge_{i=t+1}^{m} A_i$$

which is what we wanted to show. □

Theorem 12 *Let* $\bigwedge_{i=1}^{n} q_i$ *and* $\bigwedge_{i=1}^{n} q_{j_i}$ *be completely balanced formulas, where* n *is a power of two, say* $n = 2^m$*, and* $i \to j_i$ *is any permutation for* $i = 1, \ldots, n$*. Then the formula*

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{n} q_{j_i}$$

has a proof in $O(n \log^2 n)$ *symbols.*

Proof by induction on n. Suppose the theorem is true for all powers of 2 less than n. We will prove it for $n = 2^m$.

Let $\bigwedge_{i=1}^{n/2} A_i$ be an extract of $\bigwedge_{i=1}^{n} q_i$ where all the q_{j_i}'s from $i = (n/2) + 1$ to n have been removed and the parentheses kept as in $\bigwedge_{i=1}^{n} q_i$, and $\bigwedge_{i=(n/2)+1}^{n} A_i$ be an extract of $\bigwedge_{i=1}^{n} q_i$ where all the q_{j_i}'s from $i = 1$ to $n/2$ have been removed and the parentheses kept the same. Then by lemma **??** we can show

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{n/2} A_i \tag{16}$$

and

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=(n/2)+1}^{n} A_i \tag{17}$$

with $O(n \log n)$ symbols. The depth of the formulas $\bigwedge_{i=1}^{n/2} A_i$ and $\bigwedge_{i=(n/2)+1}^{n} A_i$ is at most the depth of $\bigwedge_{i=1}^{n} q_i$. i.e. at most $\log n$. By the theorem **??** the consequents of **??** and **??** can be rebalanced in $O(n \log n)$ symbols. So we can prove

$$\bigwedge_{i=1}^{n/2} A_i \supset \bigwedge_{i=1}^{n/2} A_{k_i} \tag{18}$$

and

$$\bigwedge_{i=(n/2)+1}^{n} A_i \supset \bigwedge_{i=(n/2)+1}^{n} A_{k_i} \tag{19}$$

with $O(n \log n)$ symbols, where $\bigwedge_{i=1}^{n/2} A_{k_i}$ and $\bigwedge_{i=(n/2)+1}^{n} A_{k_i}$ are completely balanced and the A_{k_i}'s are a permutation of the A_i's. Now by the induction hypothesis we can prove

$$\bigwedge_{i=1}^{n/2} A_{k_i} \supset \bigwedge_{i=1}^{n/2} q_{j_i} \tag{20}$$

and

$$\bigwedge_{i=(n/2)+1}^{n} A_{k_i} \supset \bigwedge_{i=(n/2)+1}^{n} q_{j_i} \tag{21}$$

with say $c(n/2)\log^2(n/2)$ symbols each. With $O(n)$ symbols we can prove

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{n/2} q_{j_i}$$

and

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=(n/2)+1}^{n} q_{j_i}$$

from **??**, **??** and **??**, and from **??**, **??** and **??**. Finally, with $O(n)$ more symbols we prove

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{n} q_{j_i}$$

which is what we wanted to show.

Let us now look at the total number of symbols used in this proof. Say we have used $c2(n/2)\log^2(n/2) + d_1 n \log n + d_2 n$ symbols. we will show that by taking $c \geq d_1 + d_2$, $c2(n/2)\log^2(n/2) + d_1 n \log n + d_2 n \leq cn\log^2 n$. Since $\log^2(n/2) = \log^2 n + 1 - 2\log n$,

$$\begin{aligned} & c2(n/2)\log^2(n/2) + d_1 n \log n + d_2 n \\ & \qquad \leq \quad cn\log^2 n + cn - 2cn\log n + n\log n(d_1 + d_2) \\ & \qquad \leq \quad cn\log^2 n - cn\log n + n\log n(d_1 + d_2) \\ & \qquad \leq \quad cn\log^2 n \end{aligned}$$

The result follows. □

Corollary 13 *The formula*

$$\bigwedge_{i=1}^{n} q_i \supset \bigwedge_{i=1}^{n} q_{j_i}$$

where $\bigwedge_{i=1}^{n} q_i$ *and* $\bigwedge_{i=1}^{n} q_{j_i}$ *are pseudobalanced, and* $\bigwedge_{i=1}^{n} q_{j_i}$ *is any permutation of* $\bigwedge_{i=1}^{n} q_i$*, has a proof in* $O(n\log^2 n)$ *symbols.*

Proof note that in the corollary we don't require n to be a power of 2. The result follows by two uses of lemma **??**, and one use of theorem **??**. □

5 Number of Symbols in Proofs of Transitive Closure Formulas

In this last section we are going to be working with closure formulas of the form

$$\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i}) \tag{22}$$

where both $\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i)$ and $\bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i})$ are pseudobalanced, and $\bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i})$ is a conjunction of implications $q_{s_i} \supset q_{t_i}$ where $s_i < t_i$.

Again we are going to be studying the length of proofs of such formulas with and without the deduction rule. As in the case of permutation formulas, by the informal argument given there, any proof of (**??**) has at least $\Omega((n+m)\log n)$ symbols (since $m \leq n^2$, $\log m \leq \log(n^2) = 2\log n$ and $O(n\log n + m\log m) = O((n+m)\log n)$). With the deduction rule, we can get a proof of (**??**) with $O((n+m)\log n)$ symbols the following way: first assume $\bigwedge\!\!\!\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i)$. Again for simplicity let n be a power of 2. Then we get

$$\bigwedge\!\!\!\bigwedge_{i=1}^{n/2}(q_{i-1} \supset q_i) \quad \text{and} \quad \bigwedge\!\!\!\bigwedge_{i=(n/2)+1}^{n}(q_{i-1} \supset q_i)$$

We undo (**??**) until we obtain

$$q_0 \supset q_1, q_1 \supset q_2, \ldots, q_{n-2} \supset q_{n-1}, q_{n-1} \supset q_n$$

This process takes $O(n\log n)$ symbols and $O(n)$ lines. By the work of Bonet-Buss [**?**, **?**, **?**], we prove

$$q_{s_1} \supset q_{t_1}, q_{s_2} \supset q_{t_2}, \ldots, q_{s_m} \supset q_{t_m}$$

in $O((n+m)\alpha(n))$ symbols and $O((n+m)\alpha(n))$ lines, where α is the inverse of the Ackerman function. Finally we obtain $\bigwedge\!\!\!\bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i})$ in $O(m\log m)$ symbols or $O(m)$ lines. So with a total of $O(m\log m + n\log n)$ symbols and $O((n+m)\alpha(n))$ lines we obtain the formula **??**.

If we go back to theorem **??**, we see that we can prove (**??**) with at most $O((n+m)(n+m)\alpha(n))$ symbols without the deduction rule (see (**??**) and (**??**)). The main question is now whether we can prove (**??**) without the deduction rule with less than $O((n+m)^2\alpha(n))$ symbols. The answer is yes. We will prove (**??**) with $O((n+m)\log^3 n)$ symbols without the deduction rule. So we obtain a $O((n+m)\alpha(n)/\log^3 n)$ speedup over theorem **??**. It is still open whether (**??**) has a Frege-proof of $O((n+m)\log n)$ symbols.

Before we prove the main theorem, let us obtain the following lemmas:

Lemma 14 *The formulas*

$$\bigwedge\!\!\!\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge\!\!\!\bigwedge_{i=1}^{n}(q_0 \supset q_i)$$

and

$$\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge_{i=0}^{n-1}(q_i \supset q_n)$$

where n is a power of 2, the conjunctions are completely balanced, and the q_i's are atomic formulas, have Frege proofs of $O(n \log^2 n)$ symbols.

Proof by induction on n. Suppose the lemma holds for all numbers $< n$. We will prove it for n.

By the induction hypothesis the formulas

$$\bigwedge_{i=1}^{n/2}(q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{n/2}(q_0 \supset q_i) \tag{23}$$

and

$$\bigwedge_{i=(n/2)+1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge_{i=(n/2)+1}^{n}(q_{n/2} \supset q_i) \tag{24}$$

have proofs of $O((n/2)\log^2(n/2))$ symbols. Also in the next lines we are going to show how to get a proof of

$$(q_0 \supset q_{n/2}) \wedge \bigwedge_{i=(n/2)+1}^{n}(q_{n/2} \supset q_i) \supset \bigwedge_{i=(n/2)+1}^{n}(q_0 \supset q_i) \tag{25}$$

in $O(n \log n)$ symbols. We are going to do it by induction on the size of conjunctions. Assume it holds for all numbers $< n$, and let us show it for n. By the induction hypothesis the formulas

$$(q_0 \supset q_{n/2}) \wedge \bigwedge_{i=(n/2)+1}^{3n/4}(q_{n/2} \supset q_i) \supset \bigwedge_{i=(n/2)+1}^{3n/4}(q_0 \supset q_i)$$

and

$$(q_0 \supset q_{n/2}) \wedge \bigwedge_{i=(3n/4)+1}^{n}(q_{n/2} \supset q_i) \supset \bigwedge_{i=(3n/4)+1}^{n}(q_0 \supset q_i)$$

have proofs of $O((n/2)\log(n/2))$ symbols. So we can prove both of them in $cn\log(n/2) = cn\log n - cn$ symbols, where c is a constant. With extra $O(n)$

symbols we can prove

$$(q_0 \supset q_{n/2}) \wedge [\bigwedge_{i=(n/2)+1}^{3n/4} (q_{n/2} \supset q_i) \wedge \bigwedge_{i=(3n/4)+1}^{n} (q_{n/2} \supset q_i)] \supset$$
$$[\bigwedge_{i=(n/2)+1}^{3n/4} (q_0 \supset q_i) \wedge \bigwedge_{i=(3n/4)+1}^{n} (q_0 \supset q_i)]$$

which is what we wanted to prove. It is easy to see that we can prove (**??**) with $O(n \log n)$ symbols, since we used $cn \log n - cn + O(n)$ symbols.

Also we need to prove the formula

$$\bigwedge_{i=1}^{n/2}(q_0 \supset q_i) \supset (q_0 \supset q_{n/2}). \tag{26}$$

Such formula has a proof with $O(n)$ symbols. The proof by induction is left to the reader.

From (**??**) and (**??**) we can obtain the formula

$$\bigwedge_{i=1}^{n/2}(q_0 \supset q_i) \wedge \bigwedge_{(n/2)+1}^{n} (q_{n/2} \supset q_i) \supset \bigwedge_{i=(n/2)+1}^{n} (q_0 \supset q_i) \tag{27}$$

with $O(n)$ additional symbols. Also with $O(n)$ extra symbols we prove

$$\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{n}(q_0 \supset q_i)$$

from (**??**), (**??**) and (**??**). The total number of symbols used is $cn \log^2(n/2) + e_1 n \log n + e_2 n$. If $c \geq e_1 + e_2$ then $cn \log^2(n/2) + e_1 n \log n + e_2 n \leq cn \log^2 n$. □

Lemma 15 *The formula*

$$\bigwedge_{i=1}^{l}(p_i \supset X) \wedge \bigwedge_{i=1}^{l}(X \supset q_i) \supset \bigwedge_{i=1}^{l}(p_i \supset q_i)$$

has a proof with $O(l \cdot \log l)$ symbols, where X is an atomic formula.

Proof by induction on l. The proof is left to the reader.

Lemma 16 *Let* $\bigwedge\!\!\!\!\bigwedge_{i=1}^{n} q_i$ *be a completely balanced formula for* n *a power of* 2*, and* $\langle j_1, \ldots, j_s \rangle$ *be a sequence from the set* $\{1, \ldots, n\}$*. Then there is some permutation* $\langle k_1, \ldots, k_s \rangle$ *of the sequence* $\langle j_1, \ldots, j_s \rangle$*, and there is a pseudobalanced formula* $\bigwedge\!\!\!\!\bigwedge_{i=1}^{s} q_{k_i}$ *(*q_i*'s can be omitted or repeated) such that the formula*

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n} q_i \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{s} q_{k_i}$$

can be proved with $O((n+s)\log n)$ *symbols.*

Proof by induction on n. Suppose it is true for all numbers $< n$. We'll prove it for n. By the induction hypothesis the formulas

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n/2} q_i \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{t} q_{a_i}$$

and

$$\bigwedge\!\!\!\!\bigwedge_{i=(n/2)+1}^{n} q_i \supset \bigwedge\!\!\!\!\bigwedge_{i=t+1}^{s} q_{a_i}$$

have proofs of $O(((n/2)+t)\log(n/2))$ and $O(((n/2)+(s-t))\log(n/2)$ symbols, where $\langle a_1, \ldots, a_t \rangle$ is a permutation of the j_i's which are $\leq n/2$, and $\langle a_{t+1}, \ldots, a_s \rangle$ is a permutation of the j_i's which are $\geq n/2$. So the proofs have a total of $cn\log(n/2)+cs\log(n/2)$ symbols. i.e., at most $c(n+s)\log n - c(n+s)$ symbols. We can obtain the formula

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n/2} q_i \wedge \bigwedge\!\!\!\!\bigwedge_{i=(n/2)+1}^{n} q_i \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{t} q_{a_i} \wedge \bigwedge\!\!\!\!\bigwedge_{i=t+1}^{s} q_{a_i}$$

with extra $O(n+s)$ symbols. Finally we can pseudobalance the consequent with $O(n+s)$ symbols (by theorem **??**), to obtain

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n} q_i \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{s} q_{k_i}$$

The result follows. $\Box$.

Theorem 17 *Let* $\bigwedge\!\!\!\!\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i)$ *be a completely balanced formula where* n *is a power of* 2*. Let* $\langle s_1, \ldots, s_m \rangle$ *be any sequence from the set* $\{0, 1, \ldots, n-1\}$*, and* $\langle t_1, \ldots, t_m \rangle$ *be any sequence from the set* $\{1, \ldots, n\}$ *such that* $s_i < t_i$*. Then the formula*

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i})$$

has a proof with $O((n+m)\log^3 n)$ *symbols.*

Proof by induction on n. Assume it holds for all numbers $< n$. Say $m = l_1 + l_2 + l_3$ where l_1 is the number of implications for which $q_{t_i} \leq n/2$ (i.e. in the first half), l_2 is the number of implications for which $q_{s_i} \geq n/2$ (i.e. in the second half) and l_3 is the number of implications for which $q_{s_i} < n/2$ and $q_{t_i} > n/2$ (i.e. implications across $q_{n/2}$).

Let $\langle s_i t_i \rangle$ be the tuple representing the implication $s_i \supset t_i$. We can form the sequence of tuples, $\langle \langle s_1 t_1 \rangle, \ldots, \langle s_m t_m \rangle \rangle$. We can partition this sequence in three sequences: $\langle \langle a_1 b_1 \rangle, \ldots, \langle a_{l_1} b_{l_1} \rangle \rangle$ representing the implications in the first half, $\langle \langle c_1 d_1 \rangle, \ldots, \langle c_{l_2} d_{l_2} \rangle \rangle$ representing the implications in the second half, and $\langle \langle g_1 j_1 \rangle, \ldots, \langle g_{l_3} j_{l_3} \rangle \rangle$ representing the implications across $q_{n/2}$.

By the induction hypothesis we can prove

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n/2}(q_{i-1} \supset q_i) \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{l_1}(q_{a_i} \supset q_{b_i}) \tag{28}$$

and

$$\bigwedge\!\!\!\!\bigwedge_{i=(n/2)+1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{l_2}(q_{c_i} \supset q_{d_i}) \tag{29}$$

with $c((n/2)\log^3(n/2) + l_1 \log^3(n/2)) + c((n/2)\log^3(n/2) + l_2 \log^3(n/2))$ symbols, for some constant c. So with $c\log^3(n/2)(n + l_1 + l_2)$ symbols. With extra $O(n + l_1 + l_2)$ symbols we prove the following three facts:

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{n/2}(q_{i-1} \supset q_i) \wedge \bigwedge\!\!\!\!\bigwedge_{i=(n/2)+1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{l_1}(q_{a_i} \supset q_{b_i}) \wedge \bigwedge\!\!\!\!\bigwedge_{i=1}^{l_2}(q_{c_i} \supset q_{d_i})$$

from (**??**) and (**??**),

$$\bigwedge\!\!\!\!\bigwedge_{i=1}^{l_1}(q_{a_i} \supset q_{b_i}) \wedge \bigwedge\!\!\!\!\bigwedge_{i=1}^{l_2}(q_{c_i} \supset q_{d_i}) \supset \bigwedge\!\!\!\!\bigwedge_{i=1}^{l_1+l_2}(q_{e_i} \supset q_{f_i})$$

where the consequent is now pseudobalanced by theorem **??**, and the e_i's are a permutation of the a_i's and c_i's, and the f_i's are the corresponding permutation of the b_i's and d_i's, and finally,

$$\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{l_1+l_2}(q_{e_i} \supset q_{f_i}) \tag{30}$$

from the latter two statements. Say we have used $d_1(n + l_1 + l_2)$ symbols. Now we need to prove such an implication for l_3.

By lemma **??** we can prove

$$\bigwedge_{i=1}^{n/2}((q_{i-1} \supset q_i) \supset \bigwedge_{i=0}^{(n/2)-1}(q_i \supset q_{n/2}) \tag{31}$$

and

$$\bigwedge_{i=(n/2)+1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge_{i=(n/2)+1}^{n}(q_{n/2} \supset q_i) \tag{32}$$

with say $d_2(n/2)\log^2(n/2)$ symbols each. So with a total of at most $d_2 n \log^2 n$. By lemma **??** we can prove the formulas

$$\bigwedge_{i=0}^{(n/2)-1}(q_i \supset q_{n/2}) \supset \bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{n/2}) \tag{33}$$

and

$$\bigwedge_{i=(n/2)+1}^{n}(q_{n/2} \supset q_i) \supset \bigwedge_{i=1}^{l_3}(q_{n/2} \supset q_{h_i}) \tag{34}$$

with $O(((n/2) + l_3)\log(n/2))$ symbols each where the h_i's are a permutation of the j_i's. Say with at most $d_3 n \log n + 2d_3 l_3 \log n$ symbols. Also we need to obtain the formula $\bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{j_i})$. By theorem **??** and lemma **??** we can do all this in at most $O(l_3 \log^2 l_3)$ symbols, obtaining

$$\bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{n/2}) \wedge \bigwedge_{i=1}^{l_3}(q_{n/2} \supset q_{h_i}) \supset \bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{j_i}) \tag{35}$$

in say $d_4 l_3 \log^2 l_3$ symbols. And from (**??**), (**??**) and (**??**) we obtain

$$\bigwedge_{i=0}^{(n/2)-1}(q_i \supset q_{n/2}) \wedge \bigwedge_{i=(n/2)+1}^{n}(q_{n/2} \supset q_i) \supset \bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{j_i}) \tag{36}$$

with $O(n+l_3)$ symbols, as well as from (**??**), (**??**) and (**??**) we can obtain

$$\bigwedge_{i=1}^{n}((q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{j_i}) \tag{37}$$

with $O(n+l_3)$ symbols. The last two formulas are proved with $d_5(n+l_3)$ symbols, for some constant d_5. From (**??**) and (**??**) we get

$$\bigwedge_{i=1}^{n}((q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{l_1+l_2}(q_{e_i} \supset q_{f_i}) \wedge \bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{j_i}) \tag{38}$$

with $O(n+m)$ symbols. Say with $d_6(n+m)$ symbols, for some constant d_6. At this point we only need to pseudobalance the consequent of (**??**) (by theorem **??**), and give it the required order (by theorem **??**). So we prove

$$\bigwedge_{i=1}^{l_1+l_2}(q_{e_i} \supset q_{f_i}) \wedge \bigwedge_{i=1}^{l_3}(q_{g_i} \supset q_{j_i}) \supset \bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i}) \tag{39}$$

with at most say $d_7 m \log^2 m$ symbols, where the s_i's are a permutation of the e_i's and g_i's, and the t_i's are a permutation of the f_i's and j_i's. Finally from (**??**) and (**??**) we prove

$$\bigwedge_{i=1}^{n}((q_{i-1} \supset q_i) \supset \bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i})$$

with say $d_8(n+m)$ symbols, for some constant d_8.

Now we need to compute the total of symbols used. To simplify that, let us group the following terms. Let

$$e_1(n+m) = d_1(n+l_1+l_2) + d_5(n+l_3) + d_6(n+m) + d_8(n+m)$$

Also, to group $d_2 n \log^2 n$, $d_4 l_3 \log^2 l_3$ and $d_7 m \log^2 m$, consider the fact that $m \leq n^2$. Then $\log^2 m \leq \log^2(n^2) = 4\log^2 n$. Also, $\log^2 l_3 \leq 4\log^2 n$. Then let

$$\begin{aligned} e_2(n+m)\log^2 n &= d_2 n \log^2 n + 4 d_7 m \log^2 n + 4 d_4 l_3 \log^2 n \\ &= d_2 n \log^2 n + d_7 m \log^2 m + d_4 l_3 \log^2 l_3 \end{aligned}$$

So now we just need to show that

$$\begin{aligned} c(n+m)\log^3 n \geq\ & c(n+l_1+l_2)(\log^3 n - 3\log^2 n + 3\log n - 1) + \\ & e_1(n+m) + e_2(n+m)\log^2 n + d_3 n \log n + 2 d_3 l_3 \log n \end{aligned}$$

Given that if $c \geq \max(e_1, e_2, 2d_3)$ and $n \geq 4$, then

$$e_1 l_3 + 2d_3 l_3 \log n + e_2 l_3 \log^2 n \leq c l_3 \log^3 n,$$

we only need to show that,

$$\begin{aligned} c(n + l_1 + l_2) \quad \geq \quad & c(n + l_1 + l_2)(\log^3 n - 3\log^2 n + 3\log n - 1) + \\ & e_1(n + l_1 + l_2) + e_2(n + l_1 + l_2)\log^2 n + d_3 n \log n \end{aligned}$$

Since we take $c \geq \max(e_1, e_2, 2d_3)$, that is equivalent to proving that

$$c(n + l_1 + l_2)(\log^2 n + \log n + 1) \leq c(n + l_1 + l_2)(3\log^2 n - 3\log n + 1)$$

i.e. equivalent to proving that

$$\log^2 n + \log n + 1 \leq 3\log^2 n - 3\log n + 1.$$

The equation above is true for $n \geq 4$, therefore the result follows. □

In theorem **??** we assumed n was a power of 2. By padding the formula $\bigwedge\!\!\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i)$ with $\top$ to make it have the right length we can prove the result for n not a power of 2.

Corollary 18 *With $O((n+m)\log^3 n)$ symbols we can prove the formula*

$$\bigwedge\!\!\bigwedge_{i=1}^{n}(q_{i-1} \supset q_i) \supset \bigwedge\!\!\bigwedge_{i=1}^{m}(q_{s_i} \supset q_{t_i})$$

where for all i, $1 \leq i \leq m$, $s_i < t_i$.

References

[1] Maria Luisa Bonet. *The Lengths of Propositional Proofs and the Deduction Rule.* PhD thesis, U.C. Berkeley, 1991.

[2] Maria Luisa Bonet and Samuel R. Buss. The deduction rule and linear and near-linear proof simulations. Submitted for publication.

[3] Maria Luisa Bonet and Samuel R. Buss. On the serial transitive closure problem. Submitted for publication.

[4] Maria Luisa Bonet and Samuel R. Buss. On the deduction rule and the number of proof lines. In *Proceedings Sixth Annual IEEE Symposium on Logic in Computer Science*, pages 286–297, 1991.

[5] Samuel R. Buss. The undecidability of k-provability. Manuscript, to appear in *Annals of Pure and Applied Logic*, March 1989.

[6] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[7] Stephen C. Kleene. *Introduction to Metamathematics*. Wolters-Noordhoff and North-Holland, 1971.

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

[9] Thomas A. Standish. *Data Structure Techniques*. Addison-Wesley, 1980.

[10] R. Statman. Complexity of derivations from quantifier-free Horn formulae, mechanical introduction of explicit definitions, and refinement of completeness theorems. In *Logic Colloquium '86*, pages 505–517. North-Holland, 1977.