SHARPENED LOWER BOUNDS FOR CUT ELIMINATION

SAMUEL R. BUSS

Abstract. We present sharpened lower bounds on the size of cut free proofs for first-order logic. Prior lower bounds for eliminating cuts from a proof established superexponential lower bounds as a stack of exponentials, with the height of the stack proportional to the maximum depth d of the formulas in the original proof. Our new lower bounds remove the constant of proportionality, giving an exponential stack of height equal to $d - O(1)$. The proof method is based on more efficiently expressing the Gentzen-Solovay cut formulas as low depth formulas.

1. Introduction

The Gentzen cut elimination procedure is a cornerstone of mathematical logic, and is one of the primary tools for establishing the consistency of proof systems, for extracting the constructive content of proofs, and for classifying the strengths of formal systems in terms of their consistency strengths or their computational complexity. It is well-known that cut free proofs may need to be superexponentially larger than proofs that contain cut, as shown originally by Statman [20, 21] and Orevkov [14]. The present paper sharpens these lower bounds to (almost) match the known upper bounds.

All proofs considered in this paper will be Gentzen-style sequent calculus (LK) proofs in first-order logic. The *depth* of a formula is defined to be the height of a formula when viewed as a tree. The *depth* of a proof is the maximum depth of a cut formula in P. The applications in the present paper will be for proofs that have low depth endsequents, and for these proofs, the depth will equal the maximum depth of any formula in the proof. As defined below, the *height* of a proof is the maximum number of non-weak inferences along any branch in the proof.

Let the base 2 superexponential function be defined by $2_0^n = n$ and $2_{k+1}^n = 2^{2_k^n}$. The best known upper bounds on the size of proofs generated by cut elimination state that if a proof P has depth d, then P can be transformed into a cut free proof with size $2_{d+1}^{h(P)}$, where $h(P)$ is the height of P; for this see

Supported in part by NSF grant DMS-0700533. The author thanks the John Templeton Foundation for supporting his participation in the CRM Infinity Project at the Centre de Recerca Matemàtica, Barcelona, Catalonia, Spain where the the main part of this paper was written.

Orevkov [15, 16], Zhang [24, 25], and the textbook by Troelstra and Schwichtenberg [22]. Beckmann-Buss [4] give a slightly more general result that applies in the presence of non-logical axioms. Other authors have derived similar, but not quite as sharp upper bounds, including [12, 5]. Baaz and Leitsch [2, 3] have shown that better upper lower bounds hold in some special cases.

The known lower bounds for the size of cut free proofs are also superexponential. The sharpest lower bounds for the Gentzen sequent calculus state that there is a fixed constant ϵ, $0 \leq \epsilon < 1$, and proofs P of arbitrarily large depth d, such that any cut free proof Q with the same endsequent of P has size greater than $2^{h(P)}_{\epsilon d}$. The first such result was proved by Orevkov [14], who established this with $\epsilon \approx \frac{1}{4}$, in predicate logic without function symbols. Gerhardy [10] obtained $\epsilon \approx \frac{1}{2}$ for first-order logic with function symbols.

The main result of this paper is to improve the lower bound on the size of cut free proofs to obtain $\epsilon \approx 1$. More precisely, we replace the bound $2^{h(P)}_{\epsilon d}$ with the bound 2^0_{d-c}, for $c \in \mathbb{N}$ a small constant. This is nearly optimal, as $h(P) = O(d)$.

Our new lower bound also corrects an error in the literature [26], which claimed to have established an upper bound of $2^{h(P)}_{d/2}$ on the size of cut free proofs.

Our lower bound can be compared to some upper bounds and lower bounds obtained originally by Zhang [24, 25] and refined by Gerhardy [11, 10]. They prove that if n is an upper bound on the the nesting of (alternations of) quantifiers in cut formulas, then the size of a cut free proof can be bounded essentially by $2^{h(P)}_{n+2}$. (This is a somewhat simplified and weakened restatement of Zhang's and Gerhardy's upper bounds). Furthermore, Gerhardy [10] proved these constructions are essentially optimal by showing a matching lower bound based on Gentzen-Solovay inductive initial segments.

Our lower bound, like the earlier lower bounds of Statman, Orevkov, Gerhardy, and others, is based on proving that an inductive predicate I contains a large number 2^0_n. Loosely speaking, it is shown that there are short proofs of $I(2^0_n)$, but that any cut free proof of this requires superexponential size. These short proofs are based on defining inductive initial segments (which are sometimes called "inductive cuts", confusingly, since they have nothing to do with cut inferences). The method of defining inductive initial segments goes back essentially to Gentzen [8] who used it for proving transfinite induction. It became well-known from Solovay [19], who introduced it for use in bounded arithmetic. A number of other authors have also used this technique or similar ones, independently rediscovering it on at least two occasions. These include Statman [20, 21], Yessin-Volpin [23], Nelson [13], Paris-Dimitracopoulos [17], Pudlák [18], Baaz-Leitsch [1], and Gerhardy [10].

Orevkov's lower bound [14] constructs short proofs of $I(2^0_n)$, with cuts, using intermediate formulas that have depth $d = O(n)$. Our principal innovation is to improve the depth of these formulas to $n + O(1)$. Section 2 establishes notation by proving a form of Statman's and Orevkov's lower bounds, but with $\epsilon \approx \frac{1}{2}$, over

a first-order language with function symbols. This construction is taken almost directly from [18, 10]. In Section 3, we improve this to obtain our new lower bound $\epsilon \approx 1$. Section 4 outlines how to prove the same results for first-order logic without function symbols, also with $\epsilon \approx 1$.

2. Preliminaries

We begin with a short review of our formal systems, however the reader is presumed to have basic familiarity with the sequent calculus and cut elimination, as well as at least some familiarity with bounded arithmetic systems such as S^1_2 or $I\Delta_0 + \exp$. We work with a sequent calculus for classical logic over the connectives $\forall$, $\exists$, $\wedge$, $\vee$, $\supset$, and $\neg$. The logical initial sequents are $A \longrightarrow A$, for A an atomic formula. The rules of inference are as shown below.

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

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

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

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

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

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

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

$$\forall\textit{: left}\ \frac{A(t), \Gamma \longrightarrow \Delta}{(\forall x)A(x), \Gamma \longrightarrow \Delta} \qquad \forall\textit{: right}\ \frac{\Gamma \longrightarrow \Delta, A(b)}{\Gamma \longrightarrow \Delta, (\forall x)A(x)}$$

$$\exists\textit{: left}\ \frac{A(b), \Gamma \longrightarrow \Delta}{(\exists x)A(x), \Gamma \longrightarrow \Delta} \qquad \exists\textit{: right}\ \frac{\Gamma \longrightarrow \Delta, A(t)}{\Gamma \longrightarrow \Delta, (\exists x)A(x)}$$

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

The $\forall$: right and $\exists$: left inferences must satisfy the usual eigenvariable condition that b does not appear in the lower sequent.

The first six inferences are called *weak inferences*: these are needed since we treat cedents as sequences of formulas, rather than as sets or multisets of formulas. However, the *size*, $|P|$, of a proof is defined to be equal to the number of non-weak inferences. The *height* of P is denoted $h(P)$ and is the maximum number of non-weak inferences along any branch in the proof.

Definition The *depth* of a formula A is defined by

a. If A is atomic, then $\mathit{depth}(A) = 0$.
b. If A is $\neg B$, $(\exists x)B$, or $(\forall x)B$, then $A = 1 + \mathit{depth}(B)$.
c. If A is $B \circ C$ for $\circ$ one of $\vee$, $\wedge$ or $\supset$, then $\mathit{depth}(A) = 1 + \max\{\mathit{depth}(B),\ \mathit{depth}(B)\}$.

The depth of a cut inference is the depth of its cut formula. The depth of a proof P is the maximum depth of cuts appearing in P.

A *subformula* of a first-order formula ϕ is any formula that can be obtained from any sub-formula χ of ϕ by replacing the freely occurring variables in χ that were bound variables in ϕ with arbitrary terms. Thus, for example, the subformulas of $(\forall x)A(x)$ include all the subformulas of $A(t)$ for any term t. Note that the depth of a subformula of ϕ has depth $\leq \mathit{depth}(\phi)$.

We shall use a special notion for an "extended" superexponential function. Let $\vec{u}$ be a finite sequence $\vec{u} = \langle u_1, \ldots, u_k \rangle$, with $k \geq 1$. The value $2_{\vec{u}}$ is defined inductively. For $\vec{u} = \langle u_1 \rangle$, a sequence of length one, $2_{\langle u_1 \rangle} = u_1$. And, for $\vec{u} = \langle u_1, \ldots, u_k \rangle$, $2_{\vec{u}} = u_1 + 2^{2_{\langle u_2, \ldots, u_k \rangle}}$. For instance,

$$2_{\langle a,b,c,d \rangle} \ = \ a + 2^{b+2^{c+2^d}}.$$

We now review the prior superexponential lower bound for cut elimination, based on Pudlák's exposition [18], but with the better lower bound of $\epsilon \approx \frac{1}{2}$ as obtained by Gerhardy [10]. We let T be a finitely axiomatized theory of bounded arithmetic which contains a finite fragment of Cook's theory PV plus the exponential function 2^i and the superexponential functions 2_i^x and $2_{\langle \vec{u} \rangle}$. The language of T contains function symbols for sufficiently many polynomial time computable functions to formalize the needed arguments described below: this includes sequence coding, and proving simple properties about the needed polynomial time computable functions and about the exponential and superexponential functions. The theory T is axiomatized by a finite set of purely universal formulas.

T contains an additional, uninterpreted, unary predicate symbol $I(x)$, with the two axioms $I(0)$ and $(\forall x)(I(x) \supset I(Sx))$. The predicate I is not permitted in induction axioms. The predicate $I(x)$ intuitively means that induction works up to x, or that x can be reached from zero by repeatedly adding 1. Define the formula $\psi_0(x)$ to be $I(x)$, and for $i \geq 0$, define $\psi_{i+1}(x)$ to be the formula

$$(\forall y)(\psi_i(y) \supset \psi_i(y + 2^x)).$$

There are then simple proofs of

$$\psi_i(0) \qquad \text{and} \qquad \forall x(\psi_i(x) \supset \psi_i(Sx)). \tag{1}$$

These are proved for successive values of i using simple properties of zero and successor; namely, as we show below, the formulas (1) for $i = k + 1$ are proved from those for $i = k$. In addition, as we detail below, it is easy to prove that $\psi_{i+1}(x) \supset \psi_i(2^x)$.

Let Γ be the set of universal formulas that axiomatize T, including the two axioms for the predicate $I(x)$. As we describe below, the sequents $\psi_{i+1}(x) \longrightarrow \psi_i(2^x)$ can be proved with a proof of height $O(i)$ which contain cuts on only atomic formulas and on subformulas of ψ_i. Likewise, the sequent $\longrightarrow \psi_i(0)$ is proved with proofs with height $O(i)$ and with the same cut complexity. Combining these sequents with cuts, we get a proof P_ℓ of $\Gamma \longrightarrow I(2^0_\ell)$ which has height $O(i)$ and in which all cut formulas are either atomic or are subformulas of $\psi_\ell(x)$.

Let Q_ℓ be a proof with the same conclusion $\Gamma \longrightarrow I(2^0_\ell)$ as P_ℓ in which all cuts are on quantifier-free formulas. We claim that the size of Q_ℓ is $\geq 2^0_\ell$. To prove this, we modify Q_ℓ in the following fashion. Find each $\forall$:left inference in Q_ℓ, and omit this inference and instead let the auxiliary formula of the inference remain in the antecedent of that sequents and in all sequents below that sequent, down to the endsequent. For this, contractions on (formerly universal) formulas are omitted. The result is a proof Q^*_ℓ of a sequent $\Gamma^* \longrightarrow I(2^0_\ell)$ in which every formula in Γ^* is a quantifier-free substitution instance of an axiom of T. Without loss of generality, Γ^* does not contain any variables, since any variables that are present may be replaced everywhere with the constant 0. Note that the number of formulas in Γ^* is less than or equal to the number of $\forall$:right inferences in Q_i plus the number of quantifier-free axioms in the (finite) set Γ. In particular, the number of substitution instances of $I(x) \supset I(x + 1)$ in Γ^* is less than the size of Q_ℓ.

Each such substitution instance of $I(x) \supset I(x + 1)$ is a formula of the form $I(s) \supset I(s + 1)$, for s a closed term. Let $n_0 \in \mathbb{N}$ be the least integer so that no s has value equal to n_0. Of course n_0 must be less than the size of Q_ℓ. On the other hand, we claim that $n_0 \geq 2^0_\ell$. Otherwise, we could falsify the sequent $\Gamma^* \longrightarrow I(2^0_\ell)$ in the standard model of the integers by letting $I(n)$ hold for exactly the values $n \leq n_0$. It follows that the size of Q_ℓ is greater than or equal to 2^0_ℓ.

This is enough to establish the superexponential lower bound on cut free proofs. However, it is worth examining in more detail how the proof P_ℓ can be formed. First, P_ℓ derives the sequents

$$\Gamma \longrightarrow \psi_i(0) \tag{2}$$

and

$$\Gamma, \psi_i(a) \longrightarrow \psi_i(S(a)) \tag{3}$$

for $0 \leq i \leq \ell$, where a is a free variable. For $i = 0$, these are simple to prove without cuts. For the induction step, P_ℓ derives (2) with $i = k+1$ from the three sequents

(i) $\Gamma, \psi_k(a) \longrightarrow \psi_k(S(a))$,
(ii) $\Gamma \longrightarrow S(a) = a + 2^0$,
(iii) $S(a) = a + 2^0, \psi_k(S(a)) \longrightarrow \psi_k(a + 2^0)$,

using cuts on the formulas $S(a) = a + 2^0$ and $\psi_k(S(a))$ followed by an $\supset$;right and a $\forall$:right. The sequent (i) is (3) with $i = k$. Sequent (ii) is provable by a fixed size proof. And, (iii) is provable using only cuts on subformulas of ψ_k by a proof of height $O(k)$. (This last fact is readily proved by induction on the depth of ψ_k from the fact that ψ_k has depth $O(k)$.)

As the second part of the induction step, P_ℓ derives (3) for $i = k + 1$ from the sequents

(i) $\psi_{k+1}(a), \psi_k(b) \longrightarrow \psi_k(b + 2^a)$,
(ii) $\psi_{k+1}(a), \psi_k(b + 2^a) \longrightarrow \psi_k((b + 2^a) + 2^a)$,
(iii) $\Gamma \longrightarrow (b + 2^a) + 2^a = b + 2^{S(a)}$,
(iv) $(b + 2^a) + 2^a = b + 2^{S(a)}, \psi_k((b + 2^a) + 2^a) \longrightarrow \psi_k(b + 2^{S(a)})$,

using cuts on the atomic formula $(b + 2^a) + 2^a = b + 2^{S(a)}$ and the formulas $\psi_k(b + 2^a)$ and $\psi_k((b + 2^a) + 2^a)$, followed by an $\supset$:right and a $\forall$:right. Note that (i) and (ii) are readily provable by fixed proof schemes without any cuts.

After proving all the instances of (2) and (3), P_ℓ derives the sequents

$$\Gamma, \psi_{k+1}(a) \longrightarrow \psi_k(2^a) \tag{4}$$

for $0 \leq k < \ell$. This sequent is proved from the sequents

(i) $\psi_{k+1}(a), \psi_k(0) \longrightarrow \psi_k(0 + 2^a)$,
(ii) $\Gamma \longrightarrow \psi_k(0)$,
(iii) $\Gamma \longrightarrow 0 + 2^a = 2^a$,
(iv) $0 + 2^a = 2^a, \psi_k(0 + 2^a) \longrightarrow \psi_k(2^a)$

using cuts on the formulas $0 + 2^a = 2^a$, $\psi_k(0)$ and $\psi_k(0 + 2^a)$. Note that (i) is provable by a small proof with no cuts, and that (ii) is the same as (2).

Finally, P_ℓ derives $\Gamma \longrightarrow \psi_0(2^0_\ell)$ from the sequent (2) with $i = \ell$, the sequents (4) for $0 \leq i < \ell$, and the sequents

(i) $\Gamma \longrightarrow 2^{2^0_i} = 2^0_{i+1}$,
(ii) $2^{2^0_i} = 2^0_{i+1}, \psi_{\ell-i-1}(2^{2^0_i}) \longrightarrow \psi_{\ell-i-1}(2^0_{i+1})$,

using cuts on the indicated formulas.

By inspection, the height of P_ℓ is $O(\ell)$. Its depth is 2ℓ, since $\psi_\ell(0)$ is the cut formula of maximum depth. We have thus reproved, taking $d = 2\ell$, the prior results for lower bounds on cut-elimination that were described in the introduction:

Theorem 1. *There are proofs P_ℓ of sequents $\mathfrak{S}_\ell$ of depth d and height $O(d)$ such that any cut free proof of $\mathfrak{S}_\ell$ requires size $2^0_{(1/2)d}$. The formulas in $\mathfrak{S}_\ell$ are purely universal and have depth $O(1)$.*

The proof P_ℓ constructed above has exponential size because the formulas ψ_i have exponential size, $O(2^i)$. These formulas could be replaced by polynomial size formulas, as is done by Pudlák [18] using constructions from Ferrante-Rackoff [7]. They could even be made linear size using the refinements to [7] by [6]. With these modifications, P_ℓ would be polynomial size; its depth would become larger than 2ℓ, although it would still be $O(\ell)$.

3. Improved lower bounds for cut-elimination

We now improve Theorem 1 to establish the $\epsilon \approx 1$ version of the lower bounds on the size of cut-free proofs. The idea is to modify the formulas ψ_i used in P_ℓ so that they have depth $i + O(1)$ instead of depth $2i$. For this we shall prove there are formulas φ_i (equivalent to ψ_i) such that $\varphi_i(x)$ has depth $i + O(1)$, and $\varphi_0(x)$ is $I(x)$, and the formulas

$$\varphi_{i+1}(x) \leftrightarrow (\forall y)(\varphi_i(y) \supset \varphi_i(y + 2^x)) \tag{5}$$

have proofs of height $O(i)$ and depth $i + O(1)$. The proof P_ℓ can then be carried out using the φ_i's in place of the ψ_i's, and this will give the desired lower bound on cut elimination.

Although the details will be a bit complicated, the intuition behind the construction of the φ_i's is simple. The formula $\psi_i(w)$, although exponential size, has prenex form that is a Π_i-formula after like quantifiers are collapsed. Thus, $\psi_i(w)$ can be equivalently expressed as a formula $\varphi_i(w)$ of the form

$$(\forall y_0)(\exists y_1)\cdots(Qy_{i-1})R(\langle y_0, \ldots, y_{i-1}\rangle, w), \tag{6}$$

where R is a superexponential-time computable relation. We will not be able to add R as a predicate symbol to T as this seems to be precluded by the fact that the predicate symbol I cannot be used in induction axioms. However, we will be able to introduce a finite set of new predicate and function symbols to the theory T, which will enable T to define R as a constant depth formula. After doing this, the principal task is to prove that the formulas (1) with ψ_i replaced with φ_i have T-proofs of depth $i + O(1)$.

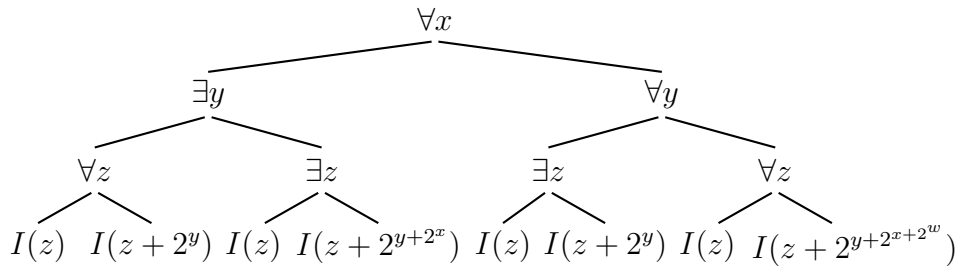
We begin by describing how to express the condition R. Recall that $\psi_0(z)$ is $I(z)$, and that $\psi_1(y)$ is $\forall z(I(z) \supset I(z + 2^y))$. Expanding further gives that $\psi_2(x)$ is

$$\forall y(\,\forall z(I(z) \supset I(z + 2^y)) \supset \forall z(I(z) \supset I(z + 2^{y+2^x}))\,),$$

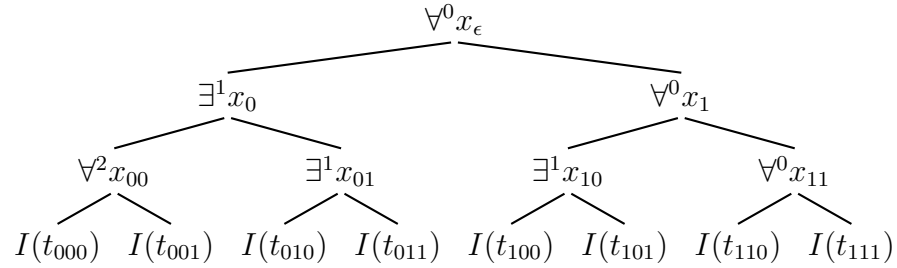
and that $\psi_3(w)$ is

$$\begin{aligned}\forall x[\,&\forall y(\,\forall z(I(z) \supset I(z + 2^y)) \supset \forall z(I(z) \supset I(z + 2^{y+2^x}))\,) \supset \\ &\forall y(\,\forall z(I(z) \supset I(z + 2^y)) \supset \forall z(I(z) \supset I(z + 2^{y+2^{x+2^w}}))\,)\,].\end{aligned}$$

To better see the pattern, consider a "skeletal" tree representation of $\psi_3(w)$.



The skeletal tree shows the quantifier structure of ψ_3, but omits the propositional connectives to keep it simpler. The skeletal tree can be written a more generic form as follows:



This is intended to represent the fact that ψ_3 is equivalent to the prenex formula

$$\forall x_\epsilon \forall x_1 \forall x_{11} \exists x_0 \exists x_{01} \exists x_{10} \forall x_{00} [((I(t_{000}) \supset I(t_{001})) \supset (I(t_{010}) \supset I(t_{011}))) \\ \supset ((I(t_{100}) \supset I(t_{101})) \supset (I(t_{110}) \supset I(t_{111})))].$$

The superscripts on the quantifiers indicate the order in which quantifiers are pulled out when putting ψ_3 in prenex form. For example, x_{11} is in the first (outermost) block of quantifiers of ψ_3's prenex form instead of the third (innermost) block.

The subscripts on the t's and x's indicate the path in the tree to reach that node, with "0" and "1" indicating left and right respectively. For instance, the term t_{011} (which is in fact the term $x_{01} + 2^{x_0+2^{x_\epsilon}}$) is reached by starting at the root and descending left, then right, then right. The empty sequence is denoted by "ϵ".

The pattern for ψ_3 generalizes to form skeletal trees of ψ_i, $i \geq 1$. The formation rules are as follows. The quantified variables in ψ_i are $x_{\vec{u}}$, for $\vec{u} \in \{0,1\}^{<i}$. The level $\ell = \ell(\vec{u})$ on the quantifier $Q^\ell x_{\vec{u}}$ is equal to the number of 0's in $\vec{u}$. A variable $x_{\vec{u}}$ is universally quantified iff its level $\ell(\vec{u})$ is even. The atomic subformulas of ψ_i are the terms $t_{\vec{u}}$ for $\vec{u} \in \{0,1\}^i$. If $\vec{v}$ is a sequence, let $|\vec{v}|$ denote the length of $\vec{v}$. For $p \leq |\vec{v}|$, let $\vec{v} \restriction p$ denote the sequence containing the first p elements of $\vec{v}$. For $t_{\vec{u}}$ a term, $\vec{u} \in \{0,1\}^i$, we define $\nu_{\vec{u}}$ to be the sequence

$$\nu_{\vec{u}} \ := \ \langle x_{\vec{u}\restriction(i-1)}, x_{\vec{u}\restriction(i-2)}, \ldots, x_{\vec{u}\restriction 1}, x_\epsilon, w \rangle,$$

namely, the variables along the path to node $\vec{u}$ plus the free variable w: this is the sequence of variables that potentially could appear in $t_{\vec{u}}$. Then, $t_{\vec{u}}$ is the

superexponential term

$$t_{\vec{u}} \ := \ 2_{\nu_{\vec{u}}\restriction(r+1)}$$

where r is the number of contiguous 1's occurring at the end of $\vec{u}$. For example, in the formula trees above, for t_{011}, there are two 1's at the end of "011", t_{011} is equal to $2_{\langle x_{01}, x_0, x_\epsilon\rangle}$, the extended superexponential function with the subscript a sequence of length $3 = r + 1$.

A variable y_ℓ in φ_i — see (6) above — will code a sequence containing the values of the variables $x_{\vec{u}}$ with level $\ell(\vec{u})$ equal to ℓ. Letting $\vec{y}$ be $\langle y_0, \ldots, y_{i-1}\rangle$, the entry y_ℓ is "well-formed" provided that it codes a function with domain equal to the set of sequences $x_{\vec{u}}$ with $|\vec{u}| < i$ and $\ell(\vec{u}) = \ell$. If y_ℓ is not well-formed, then by convention it codes the constant function which is equal to the zero on all inputs in its domain.

For $\vec{u} \in \{0,1\}^{<i}$, we write $X(\vec{u})$ to mean the value that $\vec{u}$ is mapped to by the function encoded by $\vec{y}$. (The intuition is that $X(\vec{u})$ equals the value of the variable $x_{\vec{u}}$.) We write $t(\vec{u})$ for the value of $t_{\vec{u}}$ when the variables $x_{\vec{u}'}$ are given the values $X(\vec{u}')$. Note that, although it is suppressed in the notation, $X(\vec{u})$ depends on $\vec{y}$. Also, $t(\vec{u})$ depends on both $\vec{y}$ and w, and we sometimes will write it as $t(\vec{u}, \vec{y}, w)$.

Let n be a power of two. Suppose $\vec{\sigma} \in \{T, F\}^n$, $\vec{\sigma} = \langle \sigma_0, \ldots, \sigma_{n-1}\rangle$, where T and F stand for "True" and "False". Define the relation $BIT(\vec{\sigma})$ by ("BIT" stands for "binary implication tree")

$$BIT(\vec{\sigma}) \ = \ \begin{cases} \sigma_0 & \text{if } |\vec{\sigma}| = 1 \\ BIT(\langle \sigma_0, \ldots, \sigma_{n/2-1}\rangle) \supset BIT(\langle \sigma_{n/2}, \ldots, \sigma_{n-1}\rangle) & \text{otherwise.} \end{cases}$$

We identify binary vectors $\vec{u}$ in $\{0,1\}^i$ with integers, and write $nm(\vec{u})$ for the integer with binary representation given by $\vec{u}$.

We now can define the formula $R(\vec{y}, w)$ in (6) to be

$$(\exists \vec{\sigma} \in \{0,1\}^{2^i})(BIT(\vec{\sigma}) \wedge (\forall \vec{u} \in \{0,1\}^i)[\sigma_{nm(\vec{u})} = 1 \leftrightarrow I(t(\vec{u}))]).$$

(Note that $\leftrightarrow$ is not in our first-order language; instead $A \leftrightarrow B$ is an abbreviation for $(A \supset B) \wedge (B \supset A)$.)

This completes the definition of the formulas $\varphi_i(w)$. Clearly, φ_i has depth $i + O(1)$, namely depth i plus the depth of R.

We now give a sketch of the proof that the equivalences (5) have T-proofs of depth $i + O(1)$. Note that the intuition behind the definition of R is that R states that a tree of implications holds. We define formulas S_0 and S_1 that express, respectively, the hypothesis and the conclusion of the implication, so that R is equivalent to $S_0 \supset S_1$. We do this in a general way so that we can do prenex quantifier operations with the formulas S_0 and S_1.

Suppose y_j codes a function f with domain the set of $\vec{u}$'s with $|\vec{u}| < i$ and $\ell(\vec{u}) = j$ for $j > 0$. We write $y_j /\!\!/ 0$ for the code of the function g that has as domain the set of strings $u_1 \cdots u_k$ such that $0u_1 \cdots u_k$ is in the domain of f and such that

$g(u_1 \cdots u_k) = f(0u_1 \cdots u_k)$. Define $y_j /\!\!/ 1$ similarly. For $\vec{y} = \langle y_1, \ldots, y_{i-1} \rangle$, define t_0 so that

$$t_0(\vec{u}, \langle y_0, \ldots, y_{k-1}, y_k /\!\!/ 0, \ldots, y_{i-1} /\!\!/ 0 \rangle, k)$$

is equal to $t(0\vec{u}, \langle y_0, \ldots, y_{i-1} \rangle, w)$ for all $\vec{u}$'s of length $i-1$. (Note that t_0 does not depend on w.) Likewise, define t_1 so that

$$t_1(\vec{u}, \langle y_0, \ldots, y_{k-1}, y_k /\!\!/ 1, \ldots, y_{i-1} /\!\!/ 1 \rangle, w, k)$$

is equal to $t(1\vec{u}, \langle y_0, \ldots, y_{i-1} \rangle, w)$ for all $\vec{u}$'s of length $i-1$. Let $S_0(\langle y_0, \ldots y_{i-1} \rangle, k)$ be the formula

$$(\exists \vec{\sigma} \in \{0,1\}^{2^{i-1}})(BIT(\vec{\sigma}) \wedge (\forall \vec{u} \in \{0,1\}^{i-1})[\sigma_{nm(\vec{u})} = 1 \leftrightarrow I(t_0(\vec{u}, \vec{y}, k))])$$

Let $S_1(\langle y_1, \ldots, y_{i-1} \rangle, w, k)$ be

$$(\exists \vec{\sigma} \in \{0,1\}^{2^{i-1}})(BIT(\vec{\sigma}) \wedge (\forall \vec{u} \in \{0,1\}^{i-1})[\sigma_{nm(\vec{u})} = 1 \leftrightarrow I(t_1(\vec{u}, \vec{y}, w, k))]).$$

Clearly we have $R(\vec{y}, w)$ is equivalent to $S_0(\vec{y}, w, i) \supset S_1(\vec{y}, w, i)$. And, this has a straightforward proof in the theory T.

For $k = i, i-1, \ldots, 2, 1$, consider the formulas

$$\begin{aligned}(7) \qquad (\forall y_0) \cdots (\exists y_{k-1})[(\exists y_k)(\forall y_{k+1}) \cdots (\exists y_{i-1}) S_0(\vec{y}, k) \\ \supset\ (\forall y_k)(\exists y_{k+1}) \cdots (\exists y_{i-2}) S_1(\vec{y}, w, k)],\end{aligned}$$

where the notation here assumes k and i are even (and the obvious changes are made when k or i is odd). These formulas correspond to the formulas that are obtained as $\varphi_i(w)$ is converted out of prenex form, and into a quantifier pattern that matches that of the righthand side of (5). These formulas are can be proved equivalent to each other, using proofs of size polynomial in i and using formulas that are only slightly more complicated than the formulas (7). The equivalences of the formulas (7) are proved straightforwardly by noting which parts of the (functions coded by the) variables y_ℓ are used by S_0 and S_1 and using prenex reasoning. Also, note that S_1 does not depend on y_{i-1}, so the quantifier $\forall y_{i-1}$ has been omitted in front of S_1. (The notation $\vec{y}$ thus variously denotes either $\langle y_0, \ldots, y_{i-2} \rangle$ or $\langle y_0, \ldots, y_{i-1} \rangle$, as appropriate.)

Thus, at $k = 1$, the formula

$$(8) \qquad (\forall y_0)[(\forall y_1)(\exists y_2) \cdots (\exists y_{i-1}) S_0(\vec{y}, 1) \supset (\exists y_1)(\forall y_2) \cdots (\exists y_{i-2}) S_1(\vec{y}, w, 1)]$$

is equivalent to $\varphi_i(w)$. The value y_0 codes a function with domain $1^{<i}$: y_0 can be split into two parts, the first part codes a value y_ϵ and the remaining part codes values for $f(1^j)$ for all $1 \leq j < i$. Note that S_0 depends only on the y_ϵ part of y_0. Formula (8) is thus equivalent to

$$\begin{aligned}(\forall y_\epsilon)[(\forall y_1)(\exists y_2) \cdots (\exists y_{i-1}) S_0(\langle y_\epsilon, y_1, \ldots, y_{i-1} \rangle, 1) \\ \supset\ (\forall y_0)(\exists y_1)(\forall y_2) \cdots (\exists y_{i-2}) S_1(\langle y_\epsilon \cup y_0, y_1, \ldots, y_{i-2} \rangle, w, 1)],\end{aligned}$$

where the notation $y_\epsilon \cup y_0$ denotes the number that codes the union of the functions coded by y_ϵ and y_0.

Paying attention to the way that S_1 uses w and the value y_ϵ, and letting $y_\epsilon(x)$ denote the code of the function f with domain $\{\epsilon\}$ such that $f(\epsilon) = x$, the last formula is equivalent to

$$(\forall x)[(\forall y_1)(\exists y_2)\cdots(\exists y_{i-1})S_0(\langle y_\epsilon(x), y_1, \ldots, y_{i-1}\rangle, 1) \\ \supset\ (\forall y_0)(\exists y_1)(\forall y_2)\cdots(\exists y_{i-2})S_1(\langle y_0, y_1, \ldots, y_{i-2}\rangle, w + 2^x, 0)],$$

The hypothesis of the implication is equivalent to $\varphi_{i-1}(x)$: to prove this equivalences in T, just prove that the subformulas of the hypothesis are equivalent to the corresponding subformulas of $\varphi_{i-1}(x)$ starting with the quantifier-free part, and working out to the entire formula. Similarly, the conclusion of the implication is equivalent to $\varphi_{i-1}(w + 2^x)$.

That completes the sketch of the T-proof that $\varphi_i(w)$ is equivalent to $\forall x(\varphi_{i-1}(x) \supset \varphi_{i-1}(w + 2^x))$. This, plus the lower bound on the size of Q_ℓ as established in Section 2, suffices to establish the following theorem.

Theorem 2. *There is a constant $c \in \mathbb{N}$ and proofs P_ℓ of depth $\leq \ell + c$ and height $O(\ell)$ such that every cut-free proof Q_ℓ with the same conclusion as P_ℓ has height at least 2^0_ℓ. Furthermore, the same holds for Q_ℓ containing cuts on only quantifier-free formulas.*

4. Lower bounds for relational languages

The superexponential lower bound of Theorem 2 was obtained for a language including a number of function symbols, including symbols for exponentiation and superexponentiation. The present section shows that the use of function symbols is entirely unnecessary, and the same lower bound can be obtained for a purely relational language. In prior work, Orevkov already obtained superexponential lower bounds for cut elimination in a purely relational language, but only with $\epsilon \approx \frac{1}{4}$.

The theory T used a finite set of function and relation symbols axiomatized by a set Γ of universal axioms. By standard techniques, the theory T can be converted to a purely relational theory T^{rel} with a $\forall\exists$-axiomatization. For this, each function symbol f of T is replaced by a relation symbol G_f that defines the graph of f; that is, $G_f(\vec{x}, y)$ indicates that $f(\vec{x}) = y$. The set Γ of universal axioms can be replaced by a set of axioms $\Gamma^{rel} := \Gamma_0 \cup \Gamma_1$ where Γ_0 is a set of universal axioms and Γ_1 contains the $\forall\exists$-statements asserting the totality of the functions. In particular, for each function f, Γ_1 contains the formula $(\forall\vec{x})(\exists y)G_f(\vec{x}, y)$. Γ^{rel} axiomatizes a theory T^{rel} which is equivalent to T in the sense that models of T and T^{rel} are essentially the same up to the choice of language.

The construction in the previous section of the proofs P_ℓ can be modified straightforwardly to give proofs of the corresponding statements in the new language. Formulas φ_i^{rel} that express the same condition as φ_i can be defined which still have depth $i + O(1)$ (the constant hidden in the $O(1)$ will be only slightly

larger than before). Furthermore, there are proofs of

$$\Gamma^{rel} \longrightarrow \varphi_k^{rel}(0)$$

and of

$$\Gamma, \varphi_k^{rel}(a), b = 2^a \longrightarrow \varphi_{k-1}^{rel}(b)$$

which have height $O(k)$ and depth $k + O(1)$. Here the formula "$b = 2^a$" does not use the exponential 2^a as a function, but instead is a binary relation on a and b. Combining these proofs for $1 \leq k \leq \ell$, we can form a proof P_ℓ^{rel} of height $O(\ell)$ and depth $\ell + O(1)$ of the sequent

$$\Gamma^{rel}, a_0 = 2^0, a_1 = 2^{a_0}, a_2 = 2^{a_1}, \ldots, a_\ell = 2^{a_{\ell-1}} \longrightarrow I(a_\ell).$$

Let Q_ℓ^{rel} be a cut-free proof of this sequent (or, even a proof in which all cut formulas are quantifier-free). We claim that Q_ℓ^{rel} must have size $\geq 2_\ell^0$. To prove this, we extend the lower bound argument used earlier for Q_ℓ in Section 2. This will involve (a) removing all quantifier inferences in Q_ℓ^{rel} and removing contractions on formulas that (formerly) had quantifiers, and (b) at the same time, assigning an integer value to every free variable in Q_ℓ^{rel}.

Without loss of generality, Q_ℓ^{rel} is in free variable normal form. The only free variables in the endsequent are the variables a_k, and these are assigned the integers 2_{k+1}^0. The proof Q_ℓ^{rel} is then modified iteratively by removing one quantifier inference at a time. At each stage in this process, we will have assigned integer values to all variables that occur below all quantifiers. To remove the next quantifier, choose the lowest remaining quantifier inference. If it is a $\forall$:left inference, just omit the inference, and allow the auxiliary formula in the upper sequent to remain unchanged. In addition, omit all contraction inferences on that formula and its descendants in the proof. On the other hand, suppose the lowest quantifier inference is an $\exists$:left. This will be an inference of the form

$$\frac{G_f(\vec{s}, b), \Pi \longrightarrow \Delta}{(\exists y) G_f(\vec{s}, y), \Pi \longrightarrow \Delta}$$

where $\vec{s}$ is a vector of terms and all variables in the terms in $\vec{s}$ have already been assigned integer values $\vec{n}$. Modify Q_ℓ^{rel} by omitting this $\exists$:left inference and propagating the formula $G_f(\vec{s}, b)$ down to the endsequent in place of $(\exists y) G_f(\vec{s}, y)$. The free variable b is assigned the integer value $f(\vec{n})$ so as to make $G_f(\vec{s}, b)$ true.

Once all the quantifier inferences are removed from Q_ℓ^{rel}, we obtain a proof Q_ℓ^{rel*} in which all formulas are quantifier-free. The number of substitution instances of $I(x) \supset I(Sx)$ in the antecedent of the endsequent of Q_ℓ^{rel*} is less than the size $|Q_\ell^{rel}|$ of Q_ℓ^{rel}. By a similar argument as before, this implies that $|Q_\ell^{rel}|$ is $\geq 2_\ell^0$. This gives the following lower bound for cut elimination in relational languages.

Theorem 3. *Theorem 2 holds in the purely relational language described above.*

Although our lower bounds are very close to optimal, there is still a small gap between the lower bounds of Theorems 2 and 3 and the known upper bounds discussed in the introduction. Our lower bounds have the form 2^0_ℓ. But, since P_ℓ has height $O(\ell)$ and depth $\ell + O(1)$, the upper bounds of [15, 24, 25] on the size of cut-free proofs are equal to

$$2^{O(\ell)}_{\ell+O(1)} \;=\; 2^0_{\ell+\log^*(\ell)+O(1)},$$

where $\log^*$ denotes the inverse superexponential function. It is open how to close the $\log^*$ gap between the height of superexponential size upper and lower bounds.

Acknowledgement. Wenhui Zhang provided helpful comments on an earlier draft of this paper.

References

[1] M. Baaz and A. Leitsch, *On Skolemizations and proof complexity*, Fundamenta Informaticae, 20 (1994), 353–379.
[2] ———, *Cut normal forms and proof complexity*, Annals of Pure and Applied Logic, 97 (1999), 127–177.
[3] ———, *Fast cut-elimination by CERES*. To appear in *Proofs, Categories and Computations*, College Publications, 2010.
[4] A. Beckmann and S. R. Buss, *Corrected upper bounds for free-cut elimination*. Typeset manuscript, in preparation, 2009.
[5] S. R. Buss, *An introduction to proof theory*, in Handbook of Proof Theory, S. R. Buss, ed., North-Holland, 1998, 1–78.
[6] S. R. Buss and A. Johnson, *The quantifier complexity of polynomial-size iterated definitions in first-order logic*. Typeset manuscript, 2009.
[7] J. Ferrante and C. W. Rackoff, *The Computational Complexity of Logical Theories*, Lecture Notes in Mathematics #718, Springer Verlag, Berlin, 1979.
[8] G. Gentzen, *Beweisbarkeit und Unbeweisbarkeit von Anfangsfällen der transfiniten Induktion in der reinen Zahlentheorie*, Mathematische Annalen, 119 (1943), 140–161. English translation in [9],287–308.
[9] ———, *Collected Papers of Gerhard Gentzen*, North-Holland, 1969. Edited by M. E. Szabo.
[10] P. Gerhardy, *Refined complexity analysis of cut elimination*, in Proc. 17th Workshop on Computer Science Logic (CSL), Lecture Notes in Computer Science #2803, Springer Verlag, 2003, 212–225.
[11] ———, *The role of quantifier alternations in cut elimination*, Notre Dame Journal of Formal Logic, 46 (2005), 165–171.
[12] J.-Y. Girard, *Proof Theory and Logical Complexity*, Humantities Press, 1987.
[13] E. Nelson, *Predicative Arithmetic*, Princeton University Press, 1986.
[14] V. P. Orevkov, *Lower bounds for lengthening of proofs after cut-elimination*, Journal of Soviet Mathematics, 20 (1982), 2337–2350. Original Russian version in Zap. Nauchn. Sem. L.O.M.I. Steklov **88** (1979), 137–62.
[15] ———, *Upper bound on the lengthening of proofs by cut elimination*, Journal of Soviet Mathematics, 34 (1986), pp. 1810–1819. Original Russian version in Zap. Nauchn. Sem. L.O.M.I. Steklov **137** (1984), 87–98.
[16] ———, *Applications of cut elimination to obtain estimates of proof lengths*, Soviet Mathematics Doklady, 36 (1988), 292–295. Original Russian version in Dokl. Akad. Nauk. **296**,3 (1987), 539–542.

[17] J. B. Paris and C. Dimitracopoulos, *A note on the undefinability of cuts*, Journal of Symbolic Logic, 48 (1983), 564–569.
[18] P. Pudlák, *The lengths of proofs*, in Handbook of Proof Theory, S. R. Buss, ed., Elsevier North-Holland, 1998, 547–637.
[19] R. M. Solovay. Letter to P. Hájek, August 1976.
[20] R. Statman, *Lower bounds on Herbrand's theorem*, Proceedings of the American Mathematical Society, 75 (1979), 104–107.
[21] ——, *Speed-up by theories with infinite models*, Proceedings of the American Mathematical Society, 81 (1981), 465–469.
[22] A. S. Troelstra and H. Schwichtenberg, *Basic Proof Theory*, Tracts in Theoretical Computer Science #43, Cambridge University Press, Cambridge, 2nd ed., 2000.
[23] A. S. Yessenin-Volpin, *The ultra-intuitionistic criticism and the antitraditional program for foundations of mathematics*, in Intuitionism and Proof Theory, A. Kino, J. Myhill, and R. E. Vesley, eds., North-Holland, 1970, 1–45.
[24] W. Zhang, *Cut elimination and automatic proof procedures*, Theoretical Computer Science, 91 (1991), 265–284.
[25] ——, *Depth of proofs, depth of cut-formulas, and complexity of cut formulas*, Theoretical Computer Science, 129 (1994), 193–206.
[26] ——, *Structure of proofs and the complexity of cut elimination*, Theoretical Computer Science, 353 (2006), 63–70.

Department of Mathematics
University of California, San Diego
La Jolla, CA 92093-0112, USA
E-mail address: sbuss@math.ucsd.edu