Exponential Separations between Restricted Resolution and Cutting Planes Proof Systems*

Maria Luisa Bonet[†‡] Juan Luis Esteban[§†] Nicola Galesi[¶†] Jan Johannsen[‖]

Abstract

An exponential lower bound is proved for tree-like Cutting Planes refutations of a set of clauses which has polynomial size resolution refutations. This implies an exponential separation between tree-like and dag-like proofs for both Cutting Planes and resolution; in both cases only superpolynomial separations were known before [33, 22, 11]. In order to prove this, the lower bounds on the depth of monotone circuits of Raz and McKenzie [29] are extended to monotone real circuits.

In the case of resolution, this result is further improved by giving an exponential separations of tree-like resolution from (dag-like) regular resolution as well as negative resolution proofs. In fact, the refutation provided to give the upper bound for regular resolution respects the stronger restriction of being a Davis-Putnam resolution proof. This extends the corresponding superpolynomial separation of [33].

Finally, an exponential separation between Davis-Putnam resolution and negative resolution proofs is proved; only a superpolynomial separation between Davis-Putnam and unrestricted resolution was previously known [16].

MSC2000 Classification: 03F20, 68Q17, 68T15

1 Introduction

The motivation to work on the proof length of propositional proof systems comes from two sides. First, by the work of Cook and Reckhow [13], we know that the claim that for every propositional proof system there is a class of tautologies that requires superpolynomial proof size is equivalent to $NP \neq co\text{-}NP$. This connection explains the interest in developing combinatorial techniques to prove lower bounds for different proof systems. The second motivation comes from the interest in studying efficiency issues in Automated Theorem Proving. The question is, for which proof systems are there efficient algorithms to find proofs. The most widely used proof system in implementations is resolution or restrictions of resolution. What we will show in this paper is that proving propositional proof complexity lower bounds has something to say about the non-efficiency of various strategies for finding proofs.

Haken [19] was the first who proved exponential lower bounds for unrestricted resolution. Later Urquhart [32] found another class of tautologies that require exponential size resolution proofs, and Chvátal and Szemerédi [9] showed that in some sense, almost all classes of tautologies require

*A preliminary version of this paper appeared as [6] and as ECCC TR98-035.

†Dept. Llenguatges i Sistemes Informatics, Universitat Politecnica de Catalunya, {bonet,esteban,galesi}@lsi.upc.es

‡Partially supported by projects SPRIT 20244 ALCOM-IT and TIC 97-1475-CE

§Partially supported by project KOALA:DGICYT:PB95-0787

¶Supported by an European Community grant under the TMR project

‖Dept. of Mathematics, UCSD, johannsn@math.ucsd.edu. Supported by DFG grant No. Jo 291/1-1

exponential size resolution proofs (see [3, 4] for simplified proofs of these results). These exponential lower bounds are bad news for automated theorem provers, since they mean that often the time used in finding proofs will be exponentially long in the size of the tautology, given that the shortest proofs are. The next question is, what about the classes of tautologies that have polynomial size proofs? Can we find these proofs efficiently? Several authors [3, 10, 4] have given weakly exponential time ($2^{o(n)}$) algorithms for finding resolution proofs. But, can we do better? Nothing is known at this point. Iwama [21] and Alekhnovich et al. [1] deal with a closely related question, and prove that it is NP-hard to linearly approximate the minimum resolution proof length.

Formally, we say that a propositional proof system S is *automatizable*, if there is an algorithm that for every tautology F finds a proof of F in S in time polynomial in the length of the shortest proof of F in S. The only propositional proof systems that we know are automatizable are algebraic proof systems like Hilbert's Nullstellensatz [2] and Polynomial Calculus [10]. On the other hand bounded-depth Frege proof systems are not automatizable, assuming factoring is hard [27, 8, 5]. Since Frege systems and Extended Frege systems polynomially simulate bounded-depth Frege systems, they are also not automatizable under the same assumptions.

A commonly used strategy for finding proofs is to reduce the search space by defining restricted versions of resolution that are still complete. One possibility is to restrict the system to proofs that are tree-like. Here we prove (Corollary 20) an exponential separation between tree-like resolution and resolution, showing that finding tree-like resolution proofs cannot be an efficient strategy for finding resolution proofs. Until now only superpolynomial separations were known [33, 11].

Many strategies for finding resolution proofs are described in the literature, see e.g. Schöning's textbook [31], but very little theoretical work has been done until now. Here we consider three of the most commonly used restrictions of resolution: N-resolution, Regular and Davis-Putnam resolution. We show an exponential separation between tree-like Resolution and each one of the above restrictions (Corollary 20 for N-resolution and Corollary 23 for Regular and Davis-Putnam). Goerdt [17, 16, 18] gave several superpolynomial separations between resolution and some restricted versions of it. In particular, he gave a separation between Davis-Putnam resolution and unrestricted resolution. We improve this result by giving an exponential separation between Davis-Putnam and N-resolution (Corollary 28), showing that using the Davis-Putnam restriction is not, in general, a good strategy for finding resolution proofs.

The Cutting Planes proof system (CP) is a refutation system based on manipulating integer linear inequalities for which the task of finding hard-to-prove tautologies is solved. Impagliazzo et al. [20] were the first to show such a result in the restricted case of CP proofs whose underlying graph is a tree. Bonet et al. [7] proved a lower bound for a CP system that did not have the tree-like restriction, but put a restriction in the size of the coefficients. Finally Pudlák [28] and Cook and Haken [12] gave general circuit complexity results from which a exponential lower bounds for CP follow. Nothing is known about automatizability of CP proofs. Since there is an exponential speed-up of CP over Resolution, it would be nice to find an efficient algorithm for finding CP proofs. A question to ask is if trying to find tree-like CP proofs would be an efficient strategy for finding Cutting Planes proofs.

Johannsen [22] gave a superpolynomial separation, with a lower bound of the form $\Omega(n^{\log n})$, between tree-like CP and dag-like CP (this was previously known for a restricted form of CP from [7]). Here we improve that separation to exponential (Corollary 20). This means again that trying to find tree-like proofs is not a good strategy.

This exponential separation is a consequence of extending the lower bounds of Raz and McKenzie [29] to the case of monotone real circuits. As in [29], we prove an $\Omega(n^{\epsilon})$ lower bound on the depth of monotone real circuits computing a certain monotone function GEN_n in P. This also implies an $\Omega(2^{n^\epsilon})$ lower bound on the size of monotone real formulas computing GEN_n. This latter result allows us to obtain an exponential lower bound for the size of tree-like CP proofs for a formula associated to GEN_n, using the interpolation technique of [25, 28] (Theorem 18).

The paper is organized as follows: In Section 2 we give the basic definitions of the proof systems we consider. In Section 3 we define monotone real circuits, and prove the depth lower bound for them. This is applied in Section 4 to prove the lower bounds for tree-like CP, giving exponential separations between tree-like and dag-like CP, tree-like and dag-like unrestricted Resolution as well as Regular, Davis-Putnam and N-resolution. Finally in Section 5 we prove the exponential lower bound for Davis-Putnam resolution, separating it from N-resolution. We conclude by stating some open problems.

2 The Proof Systems

Resolution is a refutation proof system for formulas in CNF based on the following inference rule:

$$\frac{C \vee x \qquad D \vee \bar{x}}{C \vee D}\ .$$

A Resolution refutation for an initial set Σ of clauses is a derivation of the empty clause from Σ using the above inference rule. Several restrictions of the resolution proof system have appeared in the literature. Here we consider the following three:

1. the *regular* resolution system, in which the proofs are restricted in such a way that any variable can be eliminated at most once in any path from an initial clause to the empty clause.

2. the *Davis-Putnam* resolution system, the subsystem of regular resolution in which the proofs are further restricted in such a way that there exists an ordering of the variables such that if a variable x is eliminated before a variable y on any path from an initial clause to the empty clause, then x is before y in the ordering. This restriction is also sometimes called *ordered* resolution in the Automated Theorem Proving community.

3. the *negative* resolution system, or N-resolution for short, where in each application of the resolution rule one of the premises must not contain any positive literals.

A proof system is *tree-like* if the proofs are restricted so that every line in a proof is used at most once as a premise of an inference. Otherwise we will call it *dag-like*.

There is an algorithm (see e.g. Urquhart [33]) that eliminates irregularities from a tree-like resolution proof, and thereby makes it smaller. Therefore tree-like resolution proofs of minimal size are regular, so tree-like resolution and tree-like regular resolution are the same proof system. This shows that tree-like resolution is a subsystem of regular resolution, and we will show that it is indeed properly weaker.

Cutting Planes (CP) is a proof system operating with linear inequalities of the form $\sum_{i \in I} a_i x_i \geq k$, where the coefficients a_i and k are integers. The rules of CP are addition of two inequalities, multiplication of an inequality by a positive integer and the following division rule:

$$\frac{\sum_{i \in I} a_i x_i \geq k}{\sum_{i \in I} \frac{a_i}{b} x_i \geq \lceil \frac{k}{b} \rceil}\ ,$$

where b is a positive integer that evenly divides all a_i, $i \in I$.

A CP refutation of a set E of inequalities is a derivation of $0 \geq 1$ from the inequalities in E and the axioms $x \geq 0$ and $-x \geq -1$ for every variable x, using the rules of CP. It can be shown that a set of inequalities has a CP-refutation iff it has no $\{0,1\}$-solution.

Cutting Planes can be used as a refutation system for propositional formulas in conjunctive normal form: note that a clause $\bigvee_{i \in P} x_i \vee \bigvee_{j \in N} \bar{x}_j$ is satisfiable iff the inequality $\sum_{i \in P} x_i - \sum_{j \in N} x_j \geq 1 - |N|$ has a $\{0,1\}$-solution. It is also well-known that CP can simulate Resolution [14], and that this simulation preserves tree-like proofs.

3 Monotone Real Circuits

A *monotone real circuit* is a circuit of fan-in 2 computing with real numbers where every gate computes a nondecreasing real function. This class of circuits was introduced by Pudlák [28]. We require that monotone real circuits output 0 or 1 on every input of zeroes and ones only, so that they are a generalization of monotone boolean circuits. The depth and size of a monotone real circuit are defined as usual, and we call it a *formula* if every gate has fan-out at most 1.

Lower bounds on the size of monotone real circuits were given by Pudlák [28], Cook and Haken [12] and Fu [15]. Rosenbloom [30] shows that they are strictly more powerful than monotone boolean circuits, since every slice function can be computed by a linear size, logarithmic depth monotone real circuit, whereas most slice functions require exponential size general boolean circuits. On the other hand, Jukna [23] gives a general lower bound criterion for monotone real circuits, and uses it to show that certain functions in $P/poly$ require exponential size monotone real circuits. Hence the computing power of monotone real circuits and general boolean circuits is incomparable.

For a monotone boolean function f, we denote by $d_{\mathbb{R}}(f)$ the minimal depth of a monotone real circuit computing f, and by $s_{\mathbb{R}}(f)$ the minimal size of a monotone real formula computing f.

The method of proving lower bounds on the depth of monotone boolean circuits using communication complexity was used by Karchmer and Wigderson [24] to give an $\Omega(\log^2 n)$ lower bound on the monotone depth of *st*-connectivity. Using the notion of real communication complexity introduced by Krajíček [26], Johannsen [22] proved the same lower bound for monotone real circuits.

The monotone function $\textsc{Gen}_n$ of n^3 inputs $t_{a,b,c}$, $1 \leq a, b, c \leq n$ is defined as follows: For $c \leq n$, we define the relation $\vdash c$ (*c is generated*) recursively by

$$\vdash c \quad \text{iff} \quad c = 1 \text{ or there are } a, b \leq n \text{ with } \vdash a\ ,\ \vdash b \text{ and } t_{a,b,c} = 1\ .$$

Finally $\textsc{Gen}_n(\vec{t}) = 1$ iff $\vdash n$. From now on we will write $a, b \vdash c$ for $t_{a,b,c} = 1$.

Recently, Raz and McKenzie [29] proved a lower bound of the form $\Omega(n^\epsilon)$ for some $\epsilon > 0$ on the depth of monotone boolean circuits computing $\textsc{Gen}_n$. We will show that their method applies to monotone real circuits:

Theorem 1 *For some $\epsilon > 0$ and sufficiently large n*

$$d_{\mathbb{R}}(\textsc{Gen}_n) \geq \Omega(n^\epsilon) \quad \textit{and} \quad s_{\mathbb{R}}(\textsc{Gen}_n) \geq 2^{\Omega(n^\epsilon)}\ .$$

3.1 Real Communication Complexity

Let $R \subseteq X \times Y \times Z$ be a multifunction, i.e. for every pair $(x, y) \in X \times Y$, there is a $z \in Z$ with $(x, y, z) \in R$. We view such a multifunction as a search problem, i.e., given input $(x, y) \in X \times Y$, the goal is to find a $z \in Z$ such that $(x, y, z) \in R$.

A real communication protocol over $X \times Y \times Z$ is executed by two players I and II who exchange information by simultaneously playing real numbers and then comparing them according to the natural order of $\mathbb{R}$. This generalizes ordinary deterministic communication protocols in the following way: in order to communicate a bit, the sender plays this bit, while the receiver plays a constant between 0 and 1, so that he can determine the value of the bit from the outcome of the comparison.

Formally, such a protocol P is specified by a binary tree, where each internal node v is labeled by two functions $f_v^I : X \to \mathbb{R}$, giving player I's move, and $f_v^{II} : Y \to \mathbb{R}$, giving player II's move, and each leaf is labeled by an element $z \in Z$. On input $(x, y) \in X \times Y$, the players construct a path through the tree according to the following rule:

> At node v, if $f_v^I(x) > f_v^{II}(y)$, then the next node is the left son of v, otherwise the right son of v.

The value $P(x, y)$ computed by P on input (x, y) is the label of the leaf reached by this path.

A real communication protocol P solves a search problem $R \subseteq X \times Y \times Z$ if for every $(x, y) \in X \times Y$, $(x, y, P(x, y)) \in R$ holds. The *real communication complexity* $CC_{\mathbb{R}}(R)$ of a search problem R is the minimal depth of a real communication protocol that solves R.

For a natural number n, let $[n]$ denote the set $\{1, \ldots, n\}$. Let $f : \{0,1\}^n \to \{0,1\}$ be a monotone boolean function, let $X := f^{-1}(1)$ and $Y := f^{-1}(0)$, and let the multifunction $R_f \subseteq X \times Y \times [n]$ be defined by

$$(x, y, i) \in R_f \quad \text{iff} \quad x_i = 1 \text{ and } y_i = 0$$

The Karchmer-Wigderson game for f is defined as follows: Player I receives an input $x \in X$ and Player II an input $y \in Y$. They have to agree on a position $i \in [n]$ such that $(x, y, i) \in R_f$. Sometimes we will say that R_f is the Karchmer-Wigderson game for the function f. There is a relation between the real communication complexity of R_f and the depth of a monotone real circuit or the size of a monotone real formula computing f, similar to the boolean case:

Lemma 2 (Krajíček [26]) *Let f be a monotone boolean function. Then*

$$CC_{\mathbb{R}}(R_f) \leq d_{\mathbb{R}}(f) \text{ and } CC_{\mathbb{R}}(R_f) \leq \log_{3/2} s_{\mathbb{R}}(f) .$$

For a proof see [26] or [22]. Hence to establish Theorem 1, it suffices to prove:

Theorem 3 *For some $\epsilon > 0$ and sufficiently large n*

$$CC_{\mathbb{R}}(R_{\mathrm{GEN}_n}) \geq \Omega(n^\epsilon).$$

3.2 DART games and structured protocols

Raz and McKenzie [29] introduced a special kind of communication games, called DART games, and a special class of communication protocols, the *structured protocols*, for solving them.

For $m, k \in \mathbb{N}$, the set of communication games $\mathrm{DART}(m, k)$ is defined as follows:

- $X = [m]^k$. I.e., the inputs for Player I are k-tuples of elements $x_i \in [m]$.
- $Y = (\{0,1\}^m)^k$. I.e., the inputs for Player II are k-tuples of binary colorings y_i of $[m]$.
- For all $i = 1, \ldots, k$ let $e_i = y_i(x_i)$. The relation $R \subseteq X \times Y \times Z$ defining the game only depends on $e_1, \ldots, e_k$ and z, i.e., we can describe $R(x, y, z)$ as $R((e_1, \ldots, e_k), z)$.

- $R((e_1, \ldots, e_k), z)$ is a DNF-Search-Problem, i.e., there exists a DNF-tautology F_R defined over the variables $e_1, \ldots, e_k$ such that Z is the set of terms of F_R, and $R((e_1, \ldots, e_k), z)$ holds if and only if the term z is satisfied by the assignment $(e_1, \ldots, e_k)$.

A *structured protocol* for a DART game is a communication protocol for solving the search problem R, where player I gets input $x \in X$, player II gets input $y \in Y$, and in each round, player I reveals the value x_i for some i, and II replies with $y_i(x_i)$. The structured communication complexity of $R \in \mathrm{DART}(m, k)$, denoted by $SC(R)$, is the minimal number of rounds in a structured protocol solving R.

The main theorem of [29] showed that for suitable m and k, the deterministic communication complexity of a DART game cannot be much smaller than that of a structured protocol. We shall show the same for its real communication complexity. Obviously, a structured protocol solving R in r rounds can be simulated by a real communication protocol solving R in $r \cdot (\lceil \log m \rceil + 1)$ rounds. Conversely, we will prove that the following holds:

Theorem 4 *For every relation $R \in \mathrm{DART}(m, k)$, where $m \geq k^{14}$,*

$$CC_{\mathbb{R}}(R) \geq SC(R) \cdot \Omega(\log m) \ .$$

In particular, this implies that for DART games, real communication protocols are no more powerful than deterministic communication protocols.

Corollary 5 *For $R \in \mathrm{DART}(m, k)$ with $m \geq k^{14}$,*

$$CC_{\mathbb{R}}(R) = \Theta(CC(R)) \ .$$

This follows from the chain of inequalities

$$CC(R) \geq CC_{\mathbb{R}}(R) \geq SC(R) \cdot \Omega(\log m) \geq \Omega(CC(R)) \ .$$

3.3 A DART game related to GEN_n

The communication game $\mathrm{PYRGEN}(m, d)$ is defined as follows:

Let $Pyr_d := \{ (i, j) \, ; \, 1 \leq j \leq i \leq d \}$. We regard the indices as elements of Pyr_d, so that the inputs for the two players I and II are respectively sequences of elements $x_{i,j} \in [m]$ and $y_{i,j} \in \{0, 1\}^m$ with $(i, j) \in Pyr_d$, and we picture these as laid out in a pyramidal form with $(1, 1)$ at the top and (d, j), $1 \leq j \leq d$ and the bottom. The goal of the game is to find either an element colored 0 at the top of the pyramid, or an element colored 1 at the bottom of the pyramid, or an element colored 1 with the two elements below it colored 0, i.e. to find indices (i, j) such that one of the following holds:

1. $i = j = 1$ and $y_{1,1}(x_{1,1}) = 0$, or
2. $y_{i,j}(x_{i,j}) = 1$ and $y_{i+1,j}(x_{i+1,j}) = 0$ and $y_{i+1,j+1}(x_{i+1,j+1}) = 0$, or
3. $i = d$ and $y_{d,j}(x_{d,j}) = 1$.

Obviously, $\mathrm{PYRGEN}(m, d)$ is a game in $\mathrm{DART}(m, \binom{d+1}{2})$. A lower bound on the structured communication complexity of $\mathrm{PYRGEN}(m, d)$ was proved in [29]:

Lemma 6 *$SC(\mathrm{PYRGEN}(m, d)) \geq d$.*

Hence by Theorem 4, we get $CC_{\mathbb{R}}(\textsc{PyrGen}(m,d)) \geq \Omega(d \log m)$ for $m \geq d^{28}$.

The following reduction shows that the real communication complexity of the game $\textsc{PyrGen}(m,d)$ is bounded by the real communication complexity of the Karchmer-Wigderson game for $\textsc{Gen}_n$ for a suitable n. The proof of the next theorem follows the ideas of [29].

Lemma 7 *For $n := m \cdot \binom{d+1}{2} + 2$,*

$$CC_{\mathbb{R}}(\textsc{PyrGen}(m,d)) \leq CC_{\mathbb{R}}(R_{\textsc{Gen}_n}).$$

Proof: We prove that any protocol P solving the Karchmer-Wigderson game for $\textsc{Gen}_n$ can be used to solve the $\textsc{PyrGen}(m,d)$ game. From their respective inputs for the $\textsc{PyrGen}(m,d)$ game, Player I and II compute respectively a minterm and a maxterm for $\textsc{Gen}_n$ and then apply the protocol P.

We interpret the elements between 2 and $n-1$ as triples (i,j,k), where $(i,j) \in Pyr_d$ and $k \in [m]$.

Now player I computes from his input $x : Pyr_d \to [m]$ an input $\vec{t_x}$ to $\textsc{Gen}_n$ with $\textsc{Gen}_n(\vec{t_x}) = 1$ by setting the following:

$$\begin{array}{ll} 1,1 \vdash a_{d,j} & \text{for } 1 \leq j \leq d \\ a_{1,1}, a_{1,1} \vdash n & \\ a_{i+1,j}, a_{i+1,j+1} \vdash a_{i,j} & \text{for } (i,j) \in Pyr_{d-1} \end{array}$$

where $a_{i,j} := (i,j,x_{i,j})$. This completely determines $\vec{t_x}$.

Likewise Player II computes from his input $y : Pyr_d \to (2^{[m]})$ a coloring col of the elements from $[n]$ by setting $col(1) = 0$, $col(n) = 1$ and $col((i,j,k)) = y_{i,j}(k)$. From this, he computes an input $\vec{t_y}$ by setting $a,b \vdash c$ iff it is not the case that $col(c) = 1$ and $col(a) = col(b) = 0$. Obviously $\textsc{Gen}_n(\vec{t_y}) = 0$.

Playing the Karchmer-Wigderson game for $\textsc{Gen}_n$ now yields a triple (a,b,c) such that $a,b \vdash c$ in $\vec{t_x}$ and $a,b \not\vdash c$ in $\vec{t_y}$. By definition of $\vec{t_y}$, this means that $col(a) = col(b) = 0$ and $col(c) = 1$, and by definition of $\vec{t_x}$ one of the following cases must hold:

- $a = b = 1$ and $c = a_{d,j}$ for some $j \leq d$. By definition of col, $y_{d,j}(x_{d,j}) = 1$.
- $c = n$ and $a = b = a_{1,1}$. In this case, $y_{1,1}(x_{1,1}) = 0$.
- $a = a_{i+1,j}$, $b = a_{i+1,j+1}$ and $c = a_{i,j}$. Then we have $y_{i,j}(x_{i,j}) = 1$, and $y_{i+1,j}(x_{i+1,j}) = y_{i+1,j+1}(x_{i+1,j+1}) = 0$.

In either case, the players have solved $\textsc{PyrGen}(m,d)$ without any additional communication. □

Now the lower bound on $CC_{\mathbb{R}}(\textsc{PyrGen}(m,d))$ obtained from Lemma 6 and Theorem 4, together with Lemma 7 immediately imply Theorem 3 with $\epsilon = \frac{1}{30}$ by taking $m = d^{28}$.

Let $\vec{t}$ be an input to $\textsc{Gen}_n$. We say that n is generated in a depth-d pyramidal fashion by $\vec{t}$ if there is a mapping $m : Pyr_d \to [n]$ such that the following hold (recall that $a,b \vdash c$ means $t_{a,b,c} = 1$):

$$\begin{array}{ll} 1,1 \vdash m(d,j) & \text{for every } j \leq d \\ m(i+1,j), m(i+1,j+1) \vdash m(i,j) & \text{for every } (i,j) \in Pyr_{d-1} \\ m(1,1), m(1,1) \vdash n & \end{array}$$

As the reduction in the proof of Lemma 7 produces only inputs from $\textsc{Gen}_n^{-1}(1)$ which have the additional property that n is generated in a depth-d pyramidal fashion, we can state the following strengthening of Theorem 1:

Corollary 8 *Let n, d and ϵ be as above. Every monotone real formula that outputs 1 on every input to* $\textsc{Gen}_n$ *for which n is generated in a depth-d pyramidal fashion, and outputs 0 on all inputs where* $\textsc{Gen}_n$ *is 0, has to be of size $\Omega(2^{n^\epsilon})$.*

The other consequences drawn from Theorem 4 and Lemma 6 in [29] apply to monotone real circuits as well, e.g. we just state without proof the following result:

Theorem 9 *There are constants $\epsilon, c > 0$ such that for every function $d(n) \leq n^\epsilon$, there is a family of monotone functions $f_n : \{0,1\}^n \to \{0,1\}$ that can be computed by monotone boolean circuits of size $n^{O(1)}$ and depth $d(n)$, but cannot be computed by monotone real circuits of depth less than $c \cdot d(n)$.*

The method also gives a simpler proof of the lower bounds in [22], in the same way as [29] simplifies the lower bound of [24].

3.4 Proof of Theorem 4

To prove Thm. 4, we first need some combinatorial notions and results from [29]. Let $A \subseteq [m]^k$ and $1 \leq j \leq k$. For $x \in [m]^{k-1}$, let $\deg_j(x, A)$ be the number of $\xi \in [m]$ such that $(x_1, \ldots, x_{j-1}, \xi, x_j, \ldots, x_{k-1}) \in A$. Then we define

$$\begin{aligned} A[j] &:= \left\{ x \in [m]^{k-1} \,;\, \deg_j(x, A) > 0 \right\} \\ AVDEG_j(A) &:= \frac{|A|}{|A[j]|} \\ MINDEG_j(A) &:= \min_{x \in A[j]} \deg_j(x, A) \\ Thickness(A) &:= \min_{1 \leq j \leq k} MINDEG_j(A) \,. \end{aligned}$$

The following lemmas about these notions were proved in [29]:

Lemma 10 *For every $A' \subseteq A$ and $1 \leq j \leq k$,*

$$AVDEG_j(A') \geq \frac{|A'|}{|A|} AVDEG_j(A) \tag{1}$$

$$Thickness(A[j]) \geq Thickness(A) \tag{2}$$

Lemma 11 *If for every $1 \leq j \leq k$, $AVDEG_j(A) \geq \delta m$ for some $0 < \delta < 1$, then for every $\alpha > 0$ there is $A' \subseteq A$ with $|A'| \geq (1-\alpha)|A|$ and*

$$Thickness(A') \geq \frac{(1-\alpha)\delta m}{k\big(1 + \alpha^{-1} \ln(\delta^{-1})\big)} \,.$$

In particular, setting $\alpha = \frac{1}{2}$ and $\delta = 4m^{-\frac{1}{14}}$, we get

Corollary 12 *If $m \geq k^{14}$ and for every $1 \leq j \leq k$, $AVDEG_j(A) \geq 4m^{\frac{13}{14}}$, then there is $A' \subseteq A$ with $|A'| \geq \frac{1}{2}|A|$ and $Thickness(A) \geq m^{\frac{11}{14}}$.*

For a relation $R \in \mathrm{DART}(m, k)$, $A \subseteq X$ and $B \subseteq Y$, let $CC_{\mathbb{R}}(R, A, B)$ be the real communication complexity of R restricted to $A \times B$.

Fix a large $m \in \mathbb{N}$. A triple (R, A, B) is called an (α, β, ℓ)-game if $R \in \mathrm{DART}(m, k)$ for some $k \leq m^{\frac{1}{14}}$ with $SC(R) \geq \ell$, $A \subseteq X$ with $|A| \geq 2^{-\alpha}|X|$ and $Thickness(A) \geq m^{\frac{11}{14}}$, and $B \subseteq Y$ with $|B| \geq 2^{-\beta}|Y|$.

Lemma 13 *For every $\alpha, \ell \geq 0$ and $0 \leq \beta \leq m^{\frac{1}{7}}$ and every (α, β, ℓ)-game (R, A, B),*

1. *if for every $1 \leq j \leq k$, $AVDEG_j(A) \geq 8m^{\frac{13}{14}}$, then there is an $(\alpha+2, \beta+1, \ell)$-game (R', A', B') with*

$$CC_{\mathbb{R}}(R', A', B') \leq CC_{\mathbb{R}}(R, A, B) - 1 .$$

2. *if $\ell \geq 1$ and for some $1 \leq j \leq k$, $AVDEG_j(A) < 8m^{\frac{13}{14}}$, then there is an $(\alpha + 3 - \frac{\log m}{14}, \beta + 1, \ell - 1)$-game (R', A', B') with*

$$CC_{\mathbb{R}}(R', A', B') \leq CC_{\mathbb{R}}(R, A, B) .$$

To prove Theorem 3 from the lemma, we show that for every (α, β, ℓ)-game (R, A, B),

$$CC_{\mathbb{R}}(R, A, B) \geq \ell \cdot \left(\frac{\log m}{42} - \frac{4}{3}\right) - \frac{\alpha + \beta}{3} . \tag{3}$$

The case $\alpha = \beta = 0$ gives the theorem.

For $\ell = 0$ and $\beta > m^{\frac{1}{7}}$, the inequality (3) is trivial, since the right hand side gets negative for large m. We proceed inductively: Let (R, A, B) be an (α, β, ℓ)-game, and assume that (3) holds for all (α', β', ℓ')-games with $\ell' \leq \ell$ and $\beta' > \beta$. For sake of contradiction, suppose that $CC_{\mathbb{R}}(R, A, B) < \ell \cdot \left(\frac{\log m}{42} - \frac{4}{3}\right) - \frac{\alpha+\beta}{3}$. Then either for every $1 \leq j \leq k$, $AVDEG_j(A) \geq 8m^{\frac{13}{14}}$, and Lemma 13 gives an $(\alpha + 2, \beta + 1, \ell)$-game (R', A', B') with

$$\begin{aligned} CC_{\mathbb{R}}(R', A', B') &\leq CC_{\mathbb{R}}(R, A, B) - 1 \\ &< \ell \cdot \left(\frac{\log m}{42} - \frac{4}{3}\right) - \frac{(\alpha + 2) + (\beta + 1)}{3} , \end{aligned}$$

or for some $1 \leq j \leq k$, $AVDEG_j(A) < 8m^{\frac{13}{14}}$, then Lemma 13 gives an $(\alpha + 3 - \frac{\log m}{14}, \beta + 1, \ell - 1)$-game (R', A', B') with

$$\begin{aligned} CC_{\mathbb{R}}(R', A', B') &< \ell \cdot \left(\frac{\log m}{42} - \frac{4}{3}\right) - \frac{\alpha + \beta}{3} \\ &= (\ell - 1) \cdot \left(\frac{\log m}{42} - \frac{4}{3}\right) - \frac{(\alpha + 3 - \frac{\log m}{14}) + (\beta + 1)}{3} , \end{aligned}$$

both contradicting the assumption.

Proof of Lemma 13: For part 1, we first show that $CC_{\mathbb{R}}(R, A, B) > 0$. Assume otherwise, then there is a term z in the DNF tautology F_R defining R that is satisfied for every $(x, y) \in A \times B$. Therefore $y_j(x_j)$ is constant for some $1 \leq j \leq k$. If γ denote the number of possible values of x_j in elements of A, then this implies that $|B| \leq 2^{mk-\gamma}$. On the other hand, $|B| \geq 2^{mk-\beta}$, hence it follows that $\beta \geq \gamma$, which is a contradiction since $\beta \leq m^{\frac{1}{7}}$, whereas $AVDEG_j(A) \geq 8m^{\frac{13}{14}}$ implies $\gamma \geq 8m^{\frac{13}{14}}$.

Let an optimal real communication protocol solving R restricted to $A \times B$ be given. For $a \in A$ and $b \in B$, let ρ_a and σ_b be the real numbers played by I and II in the first round on input a and b, respectively. W.l.o.g. we can assume that these are $|A| + |B|$ pairwise distinct real numbers.

Now consider a $\{0, 1\}$-matrix of size $|A| \times |B|$ with columns indexed by the ρ_a and rows indexed by the σ_b, both in increasing order, and where the entry in position (ρ_a, σ_b) is 1 if $\rho_a > \sigma_b$ and 0 if $\rho_a \leq \sigma_b$. Thus this entry determines the outcome of the first round, when these numbers are played. It is now obvious that either the upper right quadrant or the lower left quadrant must form a monochromatic rectangle.

Hence there are $A^\circ \subseteq A$ and $B' \subseteq B$ with $|A^\circ| \geq \frac{1}{2}|A|$ and $|B'| \geq \frac{1}{2}|B|$ such that R restricted to $A^\circ \times B'$ can be solved by a protocol with one round fewer than the original protocol. By Lemma 10 (1), $AVDEG_j(A^\circ) \geq 4m^{\frac{13}{14}}$ for every $1 \leq j \leq k$, hence by Corollary 12 there is $A' \subseteq A^\circ$ with $|A'| \geq \frac{1}{2}|A^\circ| \geq \frac{1}{4}|A|$ and $Thickness(A') \geq m^{\frac{11}{14}}$. Thus (R, A', B') is an $(\alpha+2, \beta+1, \ell)$-game.

For part 2 we proceed like in the proof of the corresponding lemma of [29], with the numbers slightly adjusted. Assume without loss of generality that in k is the coordinate for which $AVDEG_k(A) < 8m^{\frac{13}{14}}$. Let R_0 and R_1 be the restrictions of R in which the k-th coordinate $e_k = y_k(x_k)$ is fixed to 0 and 1, respectively. Obviously, R_0 and R_1 are $DART(m, k-1)$ relations, and therefore at least one of $SC(R_0)$ and $SC(R_1)$ is at least $k-1$. Assume without loss of generality that $SC(R_0) \geq k-1$. We will prove that there are two sets $A' \subseteq [m]^{k-1}$ and $B' \subseteq (\{0,1\}^m)^{k-1}$ such that the following properties hold:

$$|A'| \geq \frac{m^{k-1}}{2^{\alpha+3-\frac{\log m}{14}}} \tag{4}$$

$$|B'| \geq \frac{2^{m(k-1)}}{2^{\beta+1}} \tag{5}$$

$$Thickness(A') \geq m^{\frac{11}{14}} \tag{6}$$

$$CC_{\mathbb{R}}(R_0, A', B') \leq CC_{\mathbb{R}}(R, A, B) \tag{7}$$

This means that there is a $(\alpha+3-\frac{\log m}{14}, \beta+1, k-1)$-game (R_0, A', B') such that $CC_{\mathbb{R}}(R_0, A', B') \leq CC_{\mathbb{R}}(R, A, B)$ and this proves part 2 of Lemma 13.

Given any set $U \subset [m]$ consider the sets $A_U \subseteq [m]^{k-1}$ and $B_U \subseteq (\{0,1\}^m)^{k-1}$ associated to the set U by the following definition of [29]:

- $(x_1, \ldots x_{k-1}) \in A_U$ iff there is an $u \in U$ such that $(x_1, \ldots x_{k-1}, u) \in A$;
- $(y_1, \ldots y_{k-1}) \in B_U$ iff there is a $w \in \{0,1\}^m$ such that $w(u) = 0$ for all $u \in U$ and $(y_1, \ldots y_{k-1}, w) \in B$.

The following two claims can be proved exactly as the corresponding Claims of [29] and we omit their proof.

Claim 14 *For a random set U of size $m^{\frac{5}{14}}$ we have that*

$$Prob_U\left[A_U = A[k]\right] \geq \frac{3}{4} .$$

Claim 15 *For a random set U of size $m^{\frac{5}{14}}$ we have that*

$$Prob_U\left[|B_U| \geq \frac{|B|}{2^{m+1}}\right] \geq \frac{3}{4} .$$

Moreover it is immediate to see that the same reduction used in Claim 6.3 of [29] also works for the case of real communication complexity. Therefore we get:

Claim 16 *For every set $U \subset [m]$*

$$CC_{\mathbb{R}}(R_0, A_U, B_U) \leq CC_{\mathbb{R}}(R, A, B) .$$

Take a random set U which with probability greater than $\frac{1}{2}$, satisfies both the properties of Claim 14 and Claim 15, and define $A' := A_U$ and $B' := B_U$. This means that with probability at least $\frac{1}{2}$ both $A' = A[k]$ and $|B'| \geq \frac{|B|}{2^{m+1}}$ hold.

Recall that $\frac{|A|}{|A'|} = \frac{|A|}{|A[k]|} = AVDEG_k(A)$ and that, by hypothesis on Part 2 of the lemma $|\,AVDEG_k(A)| \leq 8m^{\frac{13}{14}}$. Therefore we have that

$$|A'| \geq \frac{|A|}{8m^{\frac{13}{14}}} \geq \frac{m^k}{2^\alpha 8m^{\frac{13}{14}}} = \frac{m^{k-1}}{2^{\alpha+3-\frac{\log m}{14}}} \,.$$

This proves (4). For (5) observe that by Claim 15 we have

$$|B'| \geq \frac{|B|}{2^{m+1}} \geq \frac{2^{mk}}{2^\beta 2^{m+1}} = \frac{2^{m(k-1)}}{2^{\beta+1}} \,.$$

The property (6) follows directly from Lemma 10 (2), and finally (7) follows from Claim 16. $\square$

4 Separation between tree-like and dag-like versions of Resolution and Cutting Planes

Cutting Planes refutations are linked to monotone real circuits by the following interpolation theorem due to Pudlák:

Theorem 17 (Pudlák [28]) *Let $\vec{p}, \vec{q}, \vec{r}$ be disjoint vectors of variables, and let $A(\vec{p}, \vec{q})$ and $B(\vec{p}, \vec{r})$ be sets of inequalities in the indicated variables such that the variables $\vec{p}$ either have only nonnegative coefficients in $A(\vec{p}, \vec{q})$ or have only non-positive coefficients in $B(\vec{p}, \vec{r})$.*

Suppose there is a CP refutation R of $A(\vec{p}, \vec{q}) \cup B(\vec{p}, \vec{r})$. Then there is a monotone real circuit $C(\vec{p})$ of size $O(|R|)$ such that for any vector $\vec{a} \in \{0,1\}^{|\vec{p}|}$

$$\begin{aligned} C(\vec{a}) = 0 \quad &\rightarrow \quad A(\vec{a}, \vec{q}) \text{ is unsatisfiable} \\ C(\vec{a}) = 1 \quad &\rightarrow \quad B(\vec{a}, \vec{r}) \text{ is unsatisfiable} \end{aligned}$$

Furthermore, if R is tree-like, then $C(\vec{p})$ is a monotone real formula.

We now define an unsatisfiable set of clauses related to GEN_n. The variables $p_{a,b,c}$ for $a, b, c \in [n]$ represent the input to GEN_n. Variables $q_{i,j,a}$ for $(i,j) \in Pyr_d$ and $a \in [n]$ encode a pyramid, where the element a is assigned to the position (i,j) by a certain mapping $m : Pyr_d \rightarrow [n]$ (cf. Corollary 8). Finally the variables r_a for $a \in [n]$ represent a coloring of the elements by $0, 1$ such that 1 is colored 0, n is colored 1 and the elements colored 0 are closed under generation. The set $Gen(\vec{p}, \vec{q})$ is given by (8) - (11), and $Col(\vec{p}, \vec{r})$ by (12) - (14).

$$\bigvee_{1 \leq a \leq n} q_{i,j,a} \qquad \text{for } (i,j) \in Pyr_d \tag{8}$$

$$\bar{q}_{d,j,a} \vee p_{1,1,a} \qquad \text{for } 1 \leq j \leq d \text{ and } a \in [n] \tag{9}$$

$$\bar{q}_{1,1,a} \vee p_{a,a,n} \qquad \text{for } a \in [n] \tag{10}$$

$$\bar{q}_{i+1,j,a} \vee \bar{q}_{i+1,j+1,b} \vee \bar{q}_{i,j,c} \vee p_{a,b,c} \qquad \text{for } (i,j) \in Pyr_{d-1} \text{ and } a,b,c \in [n] \tag{11}$$

$$\bar{p}_{1,1,a} \vee \bar{r}_a \qquad \text{for } a \in [n] \tag{12}$$

$$\bar{p}_{a,a,n} \vee r_a \qquad \text{for } a \in [n] \tag{13}$$

$$r_a \vee r_b \vee \bar{p}_{a,b,c} \vee \bar{r}_c \qquad \text{for } a,b,c \in [n] \tag{14}$$

If $Gen(\vec{t}, \vec{q})$ is satisfiable for a fixed vector $\vec{t} \in \{0,1\}^{n^3}$, then n is generated in a depth-d pyramidal fashion, and if $Col(\vec{t}, \vec{r})$ is satisfiable, then $\textsc{Gen}(\vec{t}) = 0$. Since the variables $\vec{p}$ occur only positively in $Gen(\vec{p}, \vec{q})$ and only negatively in $Col(\vec{p}, \vec{r})$, Theorem 17 is applicable, and the formula obtained from this application satisfies the conditions of Corollary 8. Hence we can conclude:

Theorem 18 *For some $\epsilon > 0$, every tree-like CP refutation of the clauses $Gen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$ has to be of size $2^{\Omega(n^\epsilon)}$.*

On the other hand, there are polynomial size dag-like resolution refutations of these clauses.

Theorem 19 *There are (dag-like) resolution refutations of size $n^{O(1)}$ of the clauses $Gen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$.*

Proof: First we resolve clauses (9) and (12) to get

$$\bar{q}_{d,j,c} \vee \bar{r}_c \tag{15}$$

for $1 \leq j \leq d$ and $1 \leq c \leq n$.

Now we want to derive $\bar{q}_{i,j,c} \vee \bar{r}_c$ for every $(i,j) \in Pyr_d$ and $1 \leq c \leq n$, by induction on i downward from d to 1. The induction base is just (15).

Now by induction we have

$$\bar{q}_{i+1,j,a} \vee \bar{r}_a \quad \text{and} \quad \bar{q}_{i+1,j+1,b} \vee \bar{r}_b \ ,$$

we resolve them against (14) to get $\bar{q}_{i+1,j,a} \vee \bar{q}_{i+1,j+1,b} \vee \bar{p}_{a,b,c} \vee \bar{r}_c$ for $1 \leq a, b, c \leq n$ and then resolve them against (11) and get

$$\bar{q}_{i+1,j,a} \vee \bar{q}_{i+1,j+1,b} \vee \bar{q}_{i,j,c} \vee \bar{r}_c$$

for every $1 \leq a, b \leq n$. All of these are then resolved against two instances of (8), and we get the desired $\bar{q}_{i,j,c} \vee \bar{r}_c$ for every $1 \leq c \leq n$.

Finally, we have in particular $\bar{q}_{1,1,a} \vee \bar{r}_a$ for every $1 \leq c \leq n$. We resolve them with (13) and get $\bar{q}_{1,1,a} \vee \bar{p}_{a,a,n}$ for every $1 \leq a \leq n$. These are resolved with (10) to get $\bar{q}_{1,1,a}$ for every $1 \leq a \leq n$. Finally, this clause is resolved with another instance of (10) (the one with $i = j = 1$) to get the empty clause. $\square$

It is easy to check that the above refutation is an N-resolution refutation. The following corollary is an easy consequence of the previous theorems and known simulation results.

Corollary 20 *The clauses $Gen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$ exponentially separate tree-like resolution from dag-like Resolution and (dag-like) N-resolution as well as tree-like Cutting Planes from dag-like Cutting Planes.*

The resolution refutation of $Gen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$ that appears in the proof of Theorem 19 is not regular. We do not know whether $Gen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$ has polynomial size regular resolution refutations. To obtain a separation between tree-like Resolution and Regular Resolution we will modify the clauses $Col(\vec{p}, \vec{r})$.

4.1 Separation of tree-like CP from regular resolution

The clauses $Col(\vec{p},\vec{r})$ are modified (and the modification called $RCol(\vec{p},\vec{r})$), so that $Gen(\vec{p},\vec{q}) \cup RCol(\vec{p},\vec{r})$ allow small regular resolutions, but in such a way that the lower bound proof still applies. We replace the variables r_a by $r_{a,i,D}$ for $a \in [n]$, $1 \le i \le d$ and $D \in \{L,R\}$, giving the coloring of element a, with auxiliary indices i being a row in the pyramid and D distinguishing whether an element is used as a left or right predecessor in the generation process.

The set $RCol(\vec{p},\vec{r})$ is defined as follows:

$$\bar{p}_{1,1,a} \vee \bar{r}_{a,d,D} \qquad \text{for } a \in [n] \text{ and } D \in \{L,R\} \tag{16}$$

$$\bar{p}_{a,a,n} \vee r_{a,1,D} \qquad \text{for } a \in [n] \text{ and } D \in \{L,R\} \tag{17}$$

$$r_{a,i+1,L} \vee r_{b,i+1,R} \vee \bar{p}_{a,b,c} \vee \bar{r}_{c,i,D} \qquad \text{for } i < d,\ a,b,c \in [n] \text{ and } D \in \{L,R\} \tag{18}$$

$$\bar{r}_{a,i,D} \vee r_{a,i,\bar{D}} \qquad \text{for } 1 \le i \le d \text{ and } D \in \{L,R\} \tag{19}$$

$$\bar{r}_{a,i,D} \vee r_{a,j,D} \qquad \text{for } 1 \le i,j \le d \text{ and } D \in \{L,R\} \tag{20}$$

Due to the clauses (19) and (20), the variables $r_{a,i,D}$ are equivalent for all values of the auxiliary indices i, D. Hence a satisfying assignment for $RCol(\vec{p},\vec{r})$ still codes a coloring of $[n]$ such that elements a with $1,1 \vdash a$ are colored 0, the elements b with $b,b \vdash n$ are colored 1, and the 0-colored elements are closed under generation. Hence if $RCol(\vec{t},\vec{r})$ is satisfiable, then $\text{GEN}(\vec{t}) = 0$.

Hence any interpolant for the clauses $Gen(\vec{p},\vec{q}) \cup RCol(\vec{p},\vec{r})$ satisfies the assumptions of Corollary 8, and we can conclude

Theorem 21 *Tree-like CP refutations of the clauses $Gen(\vec{p},\vec{q}) \cup RCol(\vec{p},\vec{r})$ have to be of size $2^{\Omega(n^{\epsilon})}$.*

On the other hand, we have the following upper bound on (dag-like) regular resolution refutations of these clauses:

Theorem 22 *There are (dag-like) regular resolution refutations of the clauses $Gen(\vec{p},\vec{q}) \cup RCol(\vec{p},\vec{r})$ of size $n^{O(1)}$.*

Proof: First we resolve clauses (9) and (16) to get

$$\bar{q}_{d,j,a} \vee \bar{r}_{a,d,D} \tag{21}$$

for $1 \le j \le d$, $1 \le a \le n$ and $D \in \{L,R\}$. Next we resolve (10) and (17) to get

$$\bar{q}_{1,1,a} \vee r_{a,1,D} \tag{22}$$

for $1 \le a \le n$ and $D \in \{L,R\}$. Finally, from (11) and (18) we obtain

$$\bar{q}_{i+1,j,a} \vee \bar{q}_{i+1,j+1,b} \vee \bar{q}_{i,j,c} \vee r_{a,i+1,L} \vee r_{b,i+1,R} \vee \bar{r}_{c,i,D} \tag{23}$$

for $1 \le j \le i < d$, $1 \le a,b,c \le n$ and $D \in \{L,R\}$.

Now we want to derive $\bar{q}_{i,j,a} \vee \bar{r}_{a,i,D}$ for every $(i,j) \in Pyr_d$, $1 \le a \le n$ and $D \in \{L,R\}$, by induction on i downward from d to 1. The induction base is just (21).

For the inductive step, resolve (23) against the clauses

$$\bar{q}_{i+1,j,a} \vee \bar{r}_{a,i+1,L} \quad \text{and} \quad \bar{q}_{i+1,j+1,b} \vee \bar{r}_{b,i+1,R}\ ,$$

which we have by induction, to give

$$\bar{q}_{i+1,j,a} \vee \bar{q}_{i+1,j+1,b} \vee \bar{q}_{i,j,c} \vee \bar{r}_{c,i,D}$$

for every $1 \leq a, b \leq n$.

All of these are then resolved against two instances of (8), and we get the desired $\bar{q}_{i,j,c} \vee \bar{r}_{c,i,D}$.

Finally, we have in particular $\bar{q}_{1,1,a} \vee \bar{r}_{a,1,L}$, which we resolve against (22) to get $\bar{q}_{1,1,a}$ for every $a \leq n$. From these and an instance of (8) we get the empty clause. □

Note that the refutation given in the proof of Theorem 22 is actually a Davis-Putnam refutation: It respects the following elimination order

$$\begin{array}{l} p_{1,1,1} \cdots p_{n,n,n} \\ r_{1,d,L} \;\; r_{1,d,R} \;\; \cdots \;\; r_{n,d,L} \;\; r_{n,d,R} \\ q_{1,d,1} \cdots q_{1,d,n} \cdots q_{d,d,1} \cdots q_{d,d,n} \\ r_{1,d-1,L} \cdots r_{n,d-1,R} \;\; q_{1,d-1,1} \cdots q_{d-1,d-1,n} \\ \vdots \\ r_{1,1,L} \;\; r_{1,1,R} \;\; q_{1,1,1} \cdots q_{1,1,n} \,. \end{array}$$

Corollary 23 *The clauses $Gen(\vec{p}, \vec{q}) \cup RCol(\vec{p}, \vec{r})$ exponentially separate the following proof systems: Tree-like Resolution from Regular and Davis-Putnam Resolution.*

5 Lower bound for Davis-Putnam resolutions

Goerdt [16] showed that Davis-Putnam resolution is strictly weaker than unrestricted resolution, by giving a superpolynomial lower bound (of the order $\Omega(n^{\log\log n})$) for Davis-Putnam resolutions of a certain family of clauses, that has polynomial size unrestricted resolution refutations. In this section we improve this separation to exponential, in fact, we give an exponential separation of Davis-Putnam resolution from N-resolution.

To simplify the exposition, we apply the method of [16] to the clauses based on *st*-connectivity that were used by Clote and Setzer [11]. These clauses are formed from variables $p_{\{i,j\}}$ for $0 \leq i, j \leq n+1$ which represent the edges of an undirected graph on $n+2$ nodes, with two distinguished nodes $s = 0$ and $t = n+1$. Variables $q_{i,j}$ for $0 \leq i, j \leq n+1$ code a sequence of nodes of length $n+2$. i.e. $q_{i,j}$ indicates whether j is in the ith position of the sequence. The set of clauses $A(\vec{p}, \vec{q})$, expressing that this sequence forms a path from s to t, is given by

$$\begin{array}{ll} q_{0,s}, \qquad q_{n+1,t} & \\ \bar{q}_{i,j} \vee \bar{q}_{i,k} & \text{for } 0 \leq i \leq n+1 \text{ and } 0 \leq j < k \leq n+1 \\ q_{i,1} \vee \ldots \vee q_{i,n+1} & \text{for } 1 \leq i \leq n \\ \bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee p_{\{j,k\}} & \text{for } 0 \leq i < n+1 \text{ and } j, k \leq n+1 \text{ with } j \neq k \,. \end{array}$$

Variables r_i code a coloring of the graph, and the set of clauses $B(\vec{p}, \vec{q})$, expressing that s and t have different colors and adjacent nodes have the same color, is given by

$$\bar{r}_s \,, \qquad r_t \,, \qquad r_i \vee \bar{p}_{\{i,j\}} \vee \bar{r}_j \quad \text{for } i, j \leq n+1 \text{ with } i \neq j \,.$$

We shall modify the clauses $A(\vec{p}, \vec{q})$ in such a way as to make small Davis-Putnam resolution refutations impossible, while still allowing for small unrestricted resolutions. The lower bound is then proved by a bottleneck counting argument similar to that used in [16], which is based on the original argument of [19].

The set $DP(\vec{p},\vec{q})$ is obtained from $A(\vec{p},\vec{q})$ by adding additional literals to some of the clauses. The clauses $\bar{q}_{i-1,j} \vee \bar{q}_{i,k} \vee p_{\{j,k\}}$ for $1 \le i \le \frac{n}{2}$ and $k \le \frac{n}{4}$ are replaced by

$$\bar{q}_{i',\ell} \vee \bar{q}_{i-1,j} \vee \bar{q}_{i,k} \vee p_{\{j,k\}}$$

for every $\ell \in [n+1]$, where $i' := \frac{n}{2} + 2(k-1) + 1$, and the clauses $\bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee p_{\{j,k\}}$ for $\frac{n}{2} < i \le n$ and $j \le \frac{n}{4}$ are replaced by

$$\bar{q}_{i',\ell} \vee \bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee p_{\{j,k\}}$$

for every $\ell \in [n+1]$, where $i' := 2j$. All other clauses remain unchanged.

Theorem 24 *The clauses $DP(\vec{p},\vec{q}) \cup B(\vec{p},\vec{r})$ have N-resolution refutations of size $n^{O(1)}$.*

Proof: We give an N-resolution refutation of $A(\vec{p},\vec{q}) \cup B(\vec{p},\vec{r})$ from [11] and then show how to adapt that refutation to $DP(\vec{p},\vec{q}) \cup B(\vec{p},\vec{r})$. By induction on i, we derive the clauses $\bar{q}_{i,j} \vee \bar{r}_j$ for $1 \le i \le n+1$. The base case $i = 1$ is done as follows. From $\bar{r}_0$ and $r_0 \vee \bar{p}_{\{0,k\}} \vee \bar{r}_k$ we get $\bar{r}_k \vee \bar{p}_{\{0,k\}}$, which is resolved with $\bar{q}_{0,0} \vee \bar{q}_{1,k} \vee p_{\{0,k\}}$ to produce $\bar{q}_{0,0} \vee \bar{q}_{1,k} \vee \bar{r}_k$, which is then resolved with $q_{0,0}$ to give $\bar{q}_{1,k} \vee \bar{r}_k$ as desired.

For the induction step, we need to derive auxiliary formulas. From $\bar{q}_{i,j} \vee \bar{r}_j$ and $r_j \vee \bar{p}_{\{j,k\}} \vee \bar{r}_k$, we get $\bar{q}_{i,j} \vee \bar{p}_{\{j,k\}} \vee \bar{r}_k$, which is resolved with $\bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee p_{\{j,k\}}$ giving $\bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee \bar{r}_k$. If we resolve $\bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee \bar{r}_k$ for all j, $0 \le j \le n+1$ with $q_{i,1} \vee \ldots \vee q_{i,n+1}$ we get $\bar{q}_{i+1,k} \vee \bar{r}_k$. Eventually we get $\bar{q}_{n+1,k} \vee \bar{r}_k$, in particular $\bar{q}_{n+1,n+1} \vee \bar{r}_{n+1}$, and we get the empty clause by resolving it with r_{n+1} and $q_{n+1,n+1}$.

The only difference in the case of the clauses $DP(\vec{p},\vec{q}) \cup B(\vec{p},\vec{r})$ is that sometimes instead of resolving $\bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee p_{\{j,k\}}$ with some clause φ to get φ', we will instead have to resolve φ with $\bar{q}_{i',\ell} \vee \bar{q}_{i-1,j} \vee \bar{q}_{i,k} \vee p_{\{j,k\}}$ (or $\bar{q}_{i',\ell} \vee \bar{q}_{i,j} \vee \bar{q}_{i+1,k} \vee p_{\{j,k\}}$) for $1 \le \ell \le n+1$. Now we solve the $n+1$ resulting resolvents (that have only negative literals) with the corresponding clause $q_{i',1} \vee \ldots \vee q_{i',n+1}$ to get φ'. $\square$

In particular, there are polynomial size unrestricted resolution refutations of these clauses.

Definition: A *critical assignment* α is given by the following:

- a coloring col_α such that $col_\alpha(s) = 0$ and $col_\alpha(t) = 1$. The values $\alpha(r_a)$ are assigned according to $col_\alpha(a)$.
- a graph G_α on $\{0, \ldots, n+1\}$ such that no two adjacent edges in G_α have different colors. Values $\alpha(p_{\{i,j\}})$ are assigned according to G_α.
- an index $i_\alpha \in [n]$ such that $\alpha(q_{i_\alpha,k}) = 0$ for all $k \in [n+1]$.
- a mapping $m_\alpha : [n]\backslash\{i_\alpha\} \to [n+1]$, which we extend by defining $m_\alpha(0) = s$ and $m_\alpha(n+1) = t$, such that if $m_\alpha(i)$ and $m_\alpha(i+1)$ are both defined and distinct, then $\{m_\alpha(i), m_\alpha(i+1)\}$ is an edge in G_α. Then we set $\alpha(q_{i,m_\alpha(i)}) = 1$ and $\alpha(q_{i,j}) = 0$ for all $j \ne m_\alpha(i)$, for every $i \ne i_\alpha$.

Obviously, a critical assignment satisfies all clauses from $B(\vec{p},\vec{r})$, and all clauses from $DP(\vec{p},\vec{q})$ except for $\bigvee_{j\in[n+1]} q_{i_\alpha,j}$.

Theorem 25 *For $n \ge 32$, every Davis-Putnam resolution refutation of the clauses $DP(\vec{p},\vec{q}) \cup B(\vec{p},\vec{r})$ contains at least $2^{\frac{n}{8}}$ clauses.*

Proof: For sake of simplicity, let n be divisible by 8. Let an elimination order $\langle x_1, \dots, x_N \rangle$ be given, where N is the number of variables, and a Davis-Putnam refutation R of $DP(\vec{p}, \vec{q}) \cup B(\vec{p}, \vec{r})$ respecting the elimination order.

For $i \in [n]$ and $s \leq N$, let $S(i, s) := \left\{ j \leq \frac{n}{4} ; q_{i,j} \in \{x_1, \dots, x_s\} \right\}$. Let i_0 denote the unique index such that there is an index $s_0 \leq N$ with $|S(i_0, s_0)| = \frac{n}{8}$, and for all $i \neq i_0$, $|S(i, s_0)| < \frac{n}{8}$. In other words, i_0 is the first index for which $\frac{n}{8}$ variables $q_{i_0,j}$ with $j \leq \frac{n}{4}$ are eliminated.

Let $S(i_0, s_0)$ be $\{j_1, \dots, j_{\frac{n}{8}}\}$. For each $1 \leq k \leq \frac{n}{8}$, let $i_k := \frac{n}{2} + 2(j_k - 1) + 1$ if $i_0 \leq \frac{n}{2}$, and $i_k := 2j_k$ if $i_0 > \frac{n}{2}$, and define

$$R_k := [\frac{n}{4}] \setminus S(i_k, s_0) \ ,$$

i.e., R_k is the set of those $j \leq \frac{n}{4}$ for which $q_{i_k,j}$ is eliminated later than any q_{i_0,j_ℓ} for $1 \leq \ell \leq \frac{n}{8}$. Note that $|R_k| \geq \frac{n}{8}$ by definition of i_0.

A critical assignment α is *0-critical*, if $i_\alpha = i_0$ and $m_\alpha(i_k) \in R_k$ for $1 \leq k \leq \frac{n}{8}$, and furthermore the following conditions hold

- if $i_0 \leq \frac{n}{2}$, then $\{m_\alpha(i_0 - 1), j_k\}$ is not an edge, but $\{j_k, m_\alpha(i_0 + 1)\}$ is an edge in G_α
- if $i_0 > \frac{n}{2}$, then $\{m_\alpha(i_0 + 1), j_k\}$ is not an edge, but $\{j_k, m_\alpha(i_0 - 1)\}$ is an edge in G_α

for every $1 \leq k \leq \frac{n}{8}$. The next lemma shows that there are many 0-critical assignments.

Lemma 26 *For every choice of pairwise distinct values $b_1, \dots, b_{\frac{n}{8}}$ with $b_k \in R_k$, there is a 0-critical assignment α with $m_\alpha(i_k) = b_k$ for $1 \leq k \leq \frac{n}{8}$ (the definition of the i_k's comes from the clauses $DP(\vec{p}, \vec{q})$).*

Proof: The assignment α is constructed as follows:

- For every index i such that $m_\alpha(i)$ is not defined yet, i.e. $i \neq i_0, i_1, \dots, i_{\frac{n}{8}}$, assign a value $m_\alpha(i) \neq s, t$ arbitrarily, such that
  - if $i_0 \leq \frac{n}{2}$, then $m_\alpha(i_0 - 1)$ does not occur at any other index, and $m_\alpha(i_0 - 2) \neq j_k$ for $1 \leq k \leq \frac{n}{8}$.
  - if $i_0 > \frac{n}{2}$, then $m_\alpha(i_0 + 1)$ does not occur at any other index, and $m_\alpha(i_0 + 2) \neq j_k$ for $1 \leq k \leq \frac{n}{8}$,

  and no value occurs both as $m_\alpha(i)$ for some $i < i_0$ and $m_\alpha(i')$ for some $i' > i_0$.
- Put every edge that occurs in this path, i.e. the edges $\{m_\alpha(i), m_\alpha(i+1)\}$ for all $0 \leq i \leq n$ such that $m_\alpha(i)$ and $m_\alpha(i+1)$ are both defined and distinct, into G_α, plus the edges $\{j_k, m_\alpha(i_0 \pm 1)\}$ that are required by the definition of 0-critical.
- Color every $m_\alpha(i)$ with $i < i_0$ by 0, and every other element by 1.

It is obvious from the construction that α is 0-critical. Note that the edges required by the definition of a 0-critical assignment do not connect nodes of different color, since if $i_0 \leq \frac{n}{2}$. then $i_k > i_0$, and if $i_0 > \frac{n}{2}$, then $i_k < i_0$, for every $k \leq \frac{n}{8}$. □

Now we map 0-critical assignments to certain clauses in the proof. For a 0-critical assignment α, let C_α be the first clause in R such that α does not satisfy C_α, and $\{ j ; q_{i_0,j} \text{ occurs in } C_\alpha \} = [n+1] \setminus \{j_1, \dots, j_{\frac{n}{8}}\}$. This clause exists because α determines a path through R from $\bigvee_{j \in [n+1]} q_{i_0,j}$ to the empty clause, such that α does not satisfy any clause on this path. The variables $q_{i_0,j}$

with $j \leq \frac{n}{4}$ are eliminated along that path, and $q_{i_0,j_1}, \ldots q_{i_0,j_{\frac{n}{8}}}$ are the first among them in the elimination order.

The following lemma shows that the clauses C_α have a certain complexity, which implies that the mapping $\alpha \mapsto C_\alpha$ does not map too many 0-critical assignments to the same clause.

Lemma 27 *Let α be a 0-critical assignment and $\ell_k := m_\alpha(i_k)$. Then for every $1 \leq k \leq \frac{n}{8}$, the literal $\bar{q}_{i_k,\ell_k}$ occurs in C_α.*

Proof: Let α' be the assignment defined by $\alpha'(q_{i_0,j_k}) := 1$ and $\alpha'(x) := \alpha(x)$ for all other variables x. As q_{i_0,j_k} does not occur in C_α, α' does not satisfy C_α either. If $i_0 \leq \frac{n}{2}$, then the only clause from $DP(\vec{p}, \vec{q}) \cup B(\vec{p}, \vec{r})$ not satisfied by α' is

$$\bar{q}_{i_k,\ell_k} \vee \bar{q}_{i_0-1,h} \vee \bar{q}_{i_0,j_k} \vee p_{\{h,j_k\}}$$

where $h := m_\alpha(i_0 - 1)$. Recall that by the definition of 0-critical truth assignment, $\{h, j_k\}$ is not an edge. If on the other hand $i_0 > \frac{n}{2}$, then the only clause from $DP(\vec{p}, \vec{q}) \cup B(\vec{p}, \vec{r})$ not satisfied by α' is

$$\bar{q}_{i_k,\ell_k} \vee \bar{q}_{i_0,j_k} \vee \bar{q}_{i_0+1,h'} \vee p_{\{j_k,h'\}}$$

where $h' := m_\alpha(i_0+1)$. Again $\{j_k, h'\}$ is not an edge by the definition of 0-critical truth assignment.

In both cases there is a path through R leading from the clause in question to C_α, such that α' does not satisfy any clause on that path. The variable that is eliminated in the last inference on that path must be one of the q_{i_0,j_r} for $1 \leq r \leq \frac{n}{8}$ by the definition of C_α. Since $\ell_k \in R_k$, the variable q_{i_k,ℓ_k} is later in the elimination order, so it cannot have been eliminated on that path. Therefore $\bar{q}_{i_k,\ell_k}$ still occurs in C_α. □

Now let α, β be two 0-critical assignments such that $\ell_k := m_\alpha(i_k) \neq m_\beta(i_k)$ for some $1 \leq k \leq \frac{n}{8}$, so that $\beta(q_{i_k,\ell_k}) = 0$. By Lemma 27, the literal $\bar{q}_{i_k,\ell_k}$ occurs in C_α, therefore β satisfies C_α, and hence $C_\beta \neq C_\alpha$.

By Lemma 26, there are at least $\frac{n}{8}!$ 0-critical assignments that differ in the values $m_\alpha(i_k)$. Thus R contains at least $\frac{n}{8}! \geq (\frac{n}{8e})^{(\frac{n}{8})}$ different clauses of the form C_α, which is at least $2^{(\frac{n}{8})}$ for $n \geq 32$. □

The following corollary is a direct consequence of Theorems 25 and 24.

Corollary 28 *The clauses $DP(\vec{p}, \vec{q}) \cup B(\vec{p}, \vec{r})$ exponentially separate Davis-Putnam Resolution from unrestricted Resolution and N-resolution.*

A modification similar to the one producing $DP(\vec{p}, \vec{q})$ from $A(\vec{p}, \vec{q})$ can also be applied to the clauses $Gen(\vec{p}, \vec{q})$, yielding a set $DPGen(\vec{p}, \vec{q})$. Then for the clauses $DPGen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$, an exponential lower bound for Davis-Putnam resolutions can be proved by the method of Theorem 25 (this was presented in the conference version [6] of this paper), and the N-resolution proofs of Theorem 19 can also be modified for these clauses. Thus the clauses $DPGen(\vec{p}, \vec{q}) \cup Col(\vec{p}, \vec{r})$ exponentially separate Davis-Putnam from negative resolution as well.

6 Open Problems

We would like to conclude by stating some open problems related to the topics of this paper.

1. For boolean circuits (monotone as well as general), circuit depth and formula size are essentially the same complexity measure, as they are exponentially related by the well-known Brent-Spira theorem. Is there an analogous theorem for monotone real circuits, i.e., is $d_{\mathbb{R}}(f) = \Theta(\log s_{\mathbb{R}}(f))$ for every monotone function f? This would be implied by the converse to Lemma 2, i.e., $d_{\mathbb{R}}(f) \leq CC_{\mathbb{R}}(R_f)$. Does this hold for every monotone function f?

2. The separation between tree-like and dag-like resolution was recently improved to a strongly exponential one, with a lower bound of the form $2^{n/\log n}$, by Ben-Sasson and Wigderson [4]. Can we prove the same strong separation between tree-like and dag-like CP?

3. A solution for the previous problem would follow from a strongly exponential separation of monotone real formula size from monotone circuit size. Such a strong separation is not even known for monotone *boolean* circuits.

4. Can the superpolynomial separations of regular and negative resolution from unrestricted resolution [17, 18] be improved to exponential as well? And is there an exponential speed-up of regular over Davis-Putnam resolution?

Acknowledgments

We would like to thank Ran Raz for reading a previous version of this work and discovering an error, Andreas Goerdt for sending us copies of his papers, Sam Buss for helpful discussions and finally Peter Clote for suggestions about resolution separations.

References

[1] M. Alekhnovich, S. R. Buss, S. Moran, and T. Pitassi. Minimum propositional proof length is NP-hard to linearly approximate. In J. Zlatuška, L. Brim, and J. Gruska, editors, *Mathematical Foundations of Computer Science '98*. Springer LNCS 1450, 1998.

[2] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73:1–26, 1996.

[3] P. Beame and T. Pitassi. Simplified and improved resolution lower bounds. In *Proc. 28th ACM Symposium on Theory of Computing*, 1996.

[4] E. Ben-Sasson and A. Wigderson. Short proofs are narrow — resolution made simple. To appear in *Proc. 31st ACM Symposium on Theory of Computing*, 1999.

[5] M. L. Bonet, C. Domingo, R. Gavalda, A. Maciel, and T. Pitassi. Non-automatizability of bounded-depth Frege proofs. To appear in *Proc. 14th IEEE Conference on Computational Complexity*, 1999.

[6] M. L. Bonet, J. L. Esteban, N. Galesi, and J. Johannsen. Exponential separations between restricted resolution and cutting planes proof systems. In *Proc. 39th Symposium on Foundations of Computer Science*, pages 638–647, 1998.

[7] M. L. Bonet, T. Pitassi, and R. Raz. Lower bounds for cutting planes proofs with small coefficients. *Journal of Symbolic Logic*, 62:708–728, 1997. Preliminary version in *Proc. 27th ACM Symposium on Theory of Computing*, 1995.

[8] M. L. Bonet, T. Pitassi, and R. Raz. No feasible interpolation for TC^0-Frege proofs. In *Proc. 38th Symposium on Foundations of Computer Science*, pages 254–263, 1997.

[9] V. Chvátal and E. Szemerédi. Many hard examples for resolution. *Journal of the ACM*, 35:759–768, 1988.

[10] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to find proofs of unsatisfiability. In *Proc. 28th ACM Symposium on Theory of Computing*, pages 174–183, 1996.

[11] P. Clote and A. Setzer. On PHP, st-connectivity and odd charged graphs. In P. Beame and S. R. Buss, editors, *Proof Complexity and Feasible Arithmetics*, pages 93–117. AMS DIMACS Series Vol. 39, 1998.

[12] S. Cook and A. Haken. An exponential lower bound for the size of monotone real circuits. To appear in *J. Comp. System Sciences*, 1998.

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

[14] W. Cook, C. Coullard, and G. Turán. On the complexity of cutting plane proofs. *Discrete Applied Mathematics*, 18:25–38, 1987.

[15] X. Fu. Lower bounds on sizes of cutting planes proofs for modular coloring principles. In P. Beame and S. R. Buss, editors, *Proof Complexity and Feasible Arithmetics*, pages 135–148. AMS DIMACS Series Vol. 39, 1998.

[16] A. Goerdt. Davis-Putnam resolution versus unrestricted resolution. *Annals of Mathematics and Artificial Intelligence*, 6:169–184, 1992.

[17] A. Goerdt. Unrestricted resolution versus N-resolution. *Theoretical Computer Science*, 93:159–167, 1992.

[18] A. Goerdt. Regular resolution versus unrestricted resolution. *SIAM Journal of Computing*, 22:661–683, 1993.

[19] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39:297–308, 1985.

[20] R. Impagliazzo, T. Pitassi, and A. Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Proc. 9th Symposium on Logic in Computer Science*, pages 220–228, 1994.

[21] K. Iwama. Complexity of finding short resolution proofs. In I. Prívara and P. Ružička, editors, *Mathematical Foundations of Computer Science '97*, pages 309–318. Springer LNCS 1295, 1997.

[22] J. Johannsen. Lower bounds for monotone real circuit depth and formula size and tree-like cutting planes. *Information Processing Letters*, 67:37–41, 1998.

[23] S. Jukna. Combinatorics of monotone computations. To appear in *Combinatorica*. Preliminary version available as ECCC TR98-041, 1998.

[24] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM Journal on Discrete Mathematics*, 3:255–265, 1990. Preliminary version in *Proc. 20th ACM Symposium on Theory of Computing*, 1988.

[25] J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic*, 62:457–486, 1997.

[26] J. Krajíček. Interpolation by a game. *Mathematical Logic Quarterly*, 44:450–458, 1998.

[27] J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S_2^1 and EF. *Information and Computation*, 140:82–94, 1998. Preliminary version in D. Leivant, ed., *LCC '94*, Springer LNCS 960, 1995.

[28] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *Journal of Symbolic Logic*, 62:981–998, 1997.

[29] R. Raz and P. McKenzie. Separation of the monotone NC hierarchy. In *Proc. 38th Symposium on Foundations of Computer Science*, pages 234–243, 1997.

[30] A. Rosenbloom. Monotone real circuits are more powerful than monotone boolean circuits. *Information Processing Letters*, 61:161–164, 1997.

[31] U. Schöning. *Logic for Computer Scientists.* Birkhäuser, 1989.

[32] A. Urquhart. Hard examples for resolution. *Journal of the ACM*, 34:209–219, 1987.

[33] A. Urquhart. The complexity of propositional proofs. *Bulletin of Symbolic Logic*, 1:425–467, 1995.