Separating DAG-Like and Tree-Like Proof Systems

Phuong Nguyen
University of Toronto

April 26, 2007

Abstract

We show that tree-like (Gentzen's calculus) **PK** where all cut formulas have depth at most a constant d does not simulate cut-free **PK**. Generally, we exhibit a family of sequents that have polynomial size cut-free proofs but requires superpolynomial tree-like proofs even when the cut rule is allowed on a class of cut-formulas that satisfies some plausible hardness assumption. This gives (in some cases, conditional) negative answers to several questions from a recent work of Maciel and Pitassi (LICS 2006). Our technique is inspired by the technique from Maciel and Pitassi. While the sequents used in earlier work are derived from the Pigeonhole principle, here we generalize Statman's sequents. This gives the desired separation, and at the same time provides stronger results in some cases.

1 Introduction

An issue of great interest in propositional proof complexity is the relative strength of different proof systems. For example, an important open problem is the question whether an optimal proof system exists, i.e., whether there is a proof system that simulates all other proof systems. Here $\mathcal{P}_1$ simulates $\mathcal{P}_2$ if for every tautology τ, the smallest $\mathcal{P}_1$-proof of τ is bounded by a polynomial in the size of a $\mathcal{P}_2$-proof of τ.

In the main part of this paper we consider Gentzen's sequent calculus **PK**, and in particular, subsystems of **PK** obtained by restricting the class of cut formulas (including cut-free **PK**) and the topology (i.e. tree-like or dag-like) of the proof. Thus for a constant d, d-**PK** is the subsystem of **PK** where all cut formulas have depth at most d, and tree-like d-**PK** (d-**PK***) is the subsystem of d-**PK** where a proof is presented as a tree (as opposed to a dag). (d-**PK** is called $\mathbf{ACC}^0_d$-**PK** in [MP06]. Here we follow [CN06].)

An early result regarding the relationship between these systems is Statman's Theorem [Sta78] which says that cut-free **PK*** does not simulate cut-free **PK** (see also [Bus88] and [CK02, Section 5.3]). The proof of this theorem is by

showing that there is a family of sequents that have polynomial-size proof in cut-free **PK**, while requiring superpolynomial-size proofs in cut-free $\mathbf{PK}^\star$.

It is also known [Kra94, Kra95] that $(d+1)$-$\mathbf{PK}^\star$ is equivalent to d-**PK** for formulas of depth d. In addition, it can be shown, as in [Kra94], that d-$\mathbf{PK}^\star$ is a proper subsystem of d-**PK**, because there is a family of depth d sequents whose smallest proof in d-$\mathbf{PK}^\star$ has size superpolynomial in the size of the smallest proof in d-**PK** (although both are *superpolynomial* in the length of the sequent). This shows that d-$\mathbf{PK}^\star$ is a proper subsystem of $(d+1)$-$\mathbf{PK}^\star$. The separating sequents are obtained from the Pigeonhole Principle (PHP) tautology by replacing each atom by a Sipser's function.

Moreover, it is shown [BB05] that $(d+1/2)$-$\mathbf{PK}^\star$ is a proper subsystem of $(d+1)$-$\mathbf{PK}^\star$. Here $(d+1/2)$-$\mathbf{PK}^\star$ is a restriction of $(d+1)$-$\mathbf{PK}^\star$ where the subformulas of depth 1 has logarithmic size. The separating sequents in [BB05] are obtained by combining the Ordering Principle and Sipser's functions. (The systems in [Kra94], as well as in [BB05], are slightly different from the systems defined here, but their arguments can be applied here.)

Recently, a number of (conditional and unconditional) lower bounds for tree-like proof systems are proved in [MP06] by converting a tree-like proof of a tautology into decision tree that solves the corresponding search problem. The lower bound for the proofs are derived from the lower bound for the decision tree, which in turns is based on the hardness (which is conditional in some cases) of certain functions. The decision tree model, while not really necessary, is a useful tool for the lower bound arguments.

The proofs in [Kra94, BB05] employ Hastad's Switching Lemma technique. Their results do not seem to apply to extensions of **PK** where there are modular counting connectives. On the other hand, [MP06] shows a way of obtaining lower bound for tree-like proofs based on complexity hardness assumption. Consequently, several (conditional and unconditional) separations regarding $\mathbf{PK}[m]$ as well as **G** are derived in [MP06]. (Here $\mathbf{PK}[m]$ is the extension of **PK** where there are modulo m counting connectives, and **G** [KP90, CM05] is the sequent calculus for quantified Boolean formulas.)

The hard sequent used in [MP06] is obtained from the sequents formalizing the Pigeonhole Principle by replacing each atom by a Boolean function which is hard for the class of cut formulas. Although a lower bound on the proof size of this generalization in the tree-like systems can be obtained, their sequents do not separate the tree-like systems from corresponding dag-like systems, since PHP is also known to be hard for the dag-like systems under consideration.

A question asked in [MP06] is whether lower bounds for dag-like proof systems can be derived from the lower bound for the tree-like counter-parts. So, for example, if $(d+1)$-$\mathbf{PK}^\star[m]$ polynomially simulates d-$\mathbf{PK}[m]$, then a (conditional) lower bound for d-$\mathbf{PK}[m]$ would follow from the (conditional) lower bound for $(d+1)$-$\mathbf{PK}^\star[m]$.

1.1 Our Results

We answer a question from [MP06] negatively by showing that d-$\mathbf{PK}^\star$ does not simulate *cut-free* $\mathbf{PK}$. The proof is by showing that there is a family of sequents that have polynomial-size cut-free $\mathbf{PK}$ proof, while require superpolynomial-size proof in d-$\mathbf{PK}$. Instead of using sequents that formalize PHP, we generalize Statman's sequents by replacing the atoms by formulas that are *hard* for the class of cut-formulas. It is known that Statman's sequents $\mathcal{S}_n$ require cut-free $\mathbf{PK}^\star$ proofs of size at least 2^n, but have polynomial-size cut-free $\mathbf{PK}$ proof, as well as polynomial-size 1-$\mathbf{PK}^\star$ proofs. (Statman's sequents have also been generalized [Ara96] to give separation between subsystems of $\mathbf{PK}$ obtained by limiting the *size*, as opposed to depth, of the cut formulas.)

Our proof of the lower bound is simpler than [MP06], because of the fact that the proof of the lower bound for Statman's sequents (in cut-free $\mathbf{PK}^\star$) is quite simple, compared to the lower bound proof of PHP. Here we do not go through decision tree (in fact, it is easy to show that the search problem corresponding to our sequents have small decision trees) but follow along the line of the arguments in a proof of Statman's theorem. To deal with cut formulas (of depth d), we explicitly define the notion of a *good assignment* for a sequent, and show that if a sequent has a large fraction of good assignments, then any tree-like proof of it must be large.

Another advantage of generalizing Statman's sequents is that the upper bound mentioned above for cut-free $\mathbf{PK}$ also holds for the general sequents. Also, the upper bound for 1-$\mathbf{PK}^\star$ can be modified to give upper bound of the proof for our general sequents in tree-like proof systems with a larger class of cut-formulas. These give the separation between tree-like and dag-like proof systems, as well as the separation between different tree-like systems.

The lower bounds proved here relies on the hardness of *parity*: It is known that formulas of depth d size $2^{m^{1/(d+1)}}$ compute $\mathit{parity}(x_1, \ldots, x_m)$ correctly on only a fraction of $1/2+1/2^{m^{1/(d+1)}}$ inputs. Our proof shows that under plausible hardness assumptions for other classes of formulas, our arguments can be used to derive conditional lower bound for some other systems, such as d-$\mathbf{PK}^\star[m]$ mentioned above, or the systems $\mathbf{G}_j^\star$ of quantified Boolean formulas.

1.2 Organization

In Section 2 we formally define the system $\mathbf{PK}$. Then in Section 3 we present Statman's sequents and the proof of its lower bound as well as upper bounds in appropriate proof systems. The lower bound argument is particularly important, because it provides the framework for our lower bound arguments presented in later sections.

In Section 4 we prove our main result: d-$\mathbf{PK}^\star$ does not simulate cut-free $\mathbf{PK}$, for any constant d. In Section 5 we analyze the arguments, and present a sufficient hardness assumption that can be used to derive lower bound (and thus separation) for other proof systems. In Section 6 we apply the general analysis and obtain (in some cases, conditional) separation for other systems, including

d-$\mathbf{PK}^\star[p]$, $\mathbf{G}^\star_j$.

Finally, we conclude with Section 7.

2 Gentzen's Sequent Calculus PK

Formulas are built from constants $\top$ (True), $\bot$ (False) and propositional variables $p, q, \ldots$ using parentheses (,) and the connectives $\neg$ and (binary) $\wedge$, $\vee$. We will use $\bigwedge, \bigvee$ when the order of parenthesizing is not important. A sequent has the form $A_1, \ldots, A_\ell \longrightarrow B_1, \ldots, B_k$ where A_i, B_j are formulas, and has the same semantics as $\bigvee(\neg A_i) \vee \bigvee B_j$ (the empty sequent is false).

As usual, a formula can be represented as a tree whose leaves are labeled with the *literals* $p, \neg p, \ldots$, and whose inner nodes are labeled with the connectives. The depth of a formula is the maximum number of blocks of connectives of the same type along any path from the root to a leaf. The size of a formula is the total number of all occurrences of literals and the $\wedge, \vee$ connectives. The size of a proof is the total size of all formulas appearing in it.

The logical axioms are of the form

$$A \longrightarrow A \qquad \bot \longrightarrow \qquad \longrightarrow \top$$

where A is any formula. (Note that most other treatments require that A be an atomic formula. As long as the proof size is concerned, there is no difference, upto a polynomial factor.)

The structural rules (weakening, contraction and exchange) are defined as usual. Other rules are as follows (here Γ and Δ denote finite sequences of formulas):

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

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

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

$$\textbf{cut}: \frac{\Gamma \longrightarrow \Delta, A \qquad A, \Gamma \longrightarrow \Delta}{\Gamma \longrightarrow \Delta}$$

3 Statman's Separation

In this section we present Statman's sequents, and show that they have short cut-free **PK** proofs as well as short 1-$\mathbf{PK}^\star$ proofs, but require exponential cut-free $\mathbf{PK}^\star$ (in fact, 0-$\mathbf{PK}^\star$) proofs. The materials are from [Bus88, CK02].

The proof of the lower bound for cut-free $\mathbf{PK}^\star$ (Theorem 3.1) is especially important; it provides the backbone for our arguments of the lower bounds in later sections. The proof of Theorem 3.2 below can be modified to show that our sequents presented in later sections all have short cut-free $\mathbf{PK}$ (or cut-free $\mathbf{PK}[m]$, or cut-free $\mathbf{G}$) proofs. Also, from the proof of Theorem 3.3, it can be shown that if our sequents have depth $d+1$, then they have short d-$\mathbf{PK}^\star$ proofs.

Consider the following sequent:

$$(\alpha_1 \vee \beta_1), \ldots, (\alpha_n \vee \beta_n) \longrightarrow p_n, q_n \tag{1}$$

where

$$\alpha_1 \equiv p_1, \quad \beta_1 \equiv q_1$$

$$\alpha_{i+1} \equiv \left(\bigvee_{j=1}^{i} (\neg p_j \wedge \neg q_j) \right) \vee p_{i+1}, \quad \beta_{i+1} \equiv \left(\bigvee_{j=1}^{i} (\neg p_j \wedge \neg q_j) \right) \vee q_{i+1}$$

Note that α_i, β_i have depth 2. Also,

$$\alpha_{i+1} \Leftrightarrow \left(\bigwedge_{j=1}^{i} (p_j \vee q_j) \right) \supset p_{i+1}, \quad \beta_{i+1} \Leftrightarrow \left(\bigwedge_{j=1}^{i} (p_j \vee q_j) \right) \supset q_{i+1}$$

(Note that formally our set of connectives does not include $\supset$).

Theorem 3.1. *Any cut-free* $\mathbf{PK}^\star$ *proof of the sequent* (1) *has size at least* 2^n.

Proof Idea. The proof is by induction on n. The base case ($n = 1$) is obvious: Any $\mathbf{PK}$ proof of

$$p_1 \vee q_1 \longrightarrow p_1, q_1$$

must have size at least 2.

For the induction step, suppose that the theorem is true for $n-1$. We prove it for n. Consider a cut-free $\mathbf{PK}^\star$ proof of (1). The last application of the $\vee$-left rule must be of the form

$$\frac{\Gamma, \alpha_i \longrightarrow \Delta \qquad \Gamma, \beta_i \longrightarrow \Delta}{\Gamma, \alpha_i \vee \beta_i \longrightarrow \Delta} \tag{2}$$

for some $1 \leq i \leq n$, where (viewing Γ, Δ as sets):

$$\{\alpha_1 \vee \beta_1, \ldots, \alpha_{i-1} \vee \beta_{i-1}, \alpha_{i+1} \vee \beta_{i+1}, \ldots, \alpha_n \vee \beta_n\} \subseteq \Gamma \subseteq \{\alpha_1 \vee \beta_1, \ldots, \alpha_n \vee \beta_n\}$$

and

$$\Delta = \{p_n, q_n\}$$

Now we argue that a proof of each upper sequent in (2) must be at least 2^{n-1}. Consider the following cases:

Case I: $i < n$. By setting both p_i, q_i to $\top$ (True), the sequent $\Gamma, \alpha_i \longrightarrow \Delta$ becomes essentially a sequent $\mathcal{S}'$ of the form (1) but with $2(n-1)$ variables

$$p_1, q_1, \ldots, p_{i-1}, q_{i-1}, p_{i+1}, q_{i+1}, \ldots, p_n, q_n$$

In fact, a proof of $\Gamma, \alpha_i \longrightarrow \Delta$ can be transformed to a proof of $\mathcal{S}'$ of smaller or equal size. Hence, by the induction hypothesis, a proof of $\Gamma, \alpha_i \longrightarrow \Delta$ must have size at least 2^{n-1}.

Case II: $i = n$. Here we set both p_n, q_n to $\bot$ (False). The argument is as in the previous case. Although the transformation of a proof of $\Gamma, \alpha_i \longrightarrow \Delta$ to a proof of the sequent of the form (1) (with $2(n-1)$ variables $p_1, q_1, \ldots, p_{n-1}, q_{n-1}$) is slightly more complicated, the proof is straightforward. □

The proof can be extended to show that any 0-$\mathbf{PK}^\star$ proof of (1) must have size at least 2^n. We have to consider additional cases where the last inference is a cut rule. The case where the cut formula is a constant $\bot$ or $\top$ is obvious. Otherwise, if the cut formula is in $\{p_i, q_i \neg p_i, \neg q_i\}$, then we can use the same arguments as in **Case I** or **Case II** above.

Now we show that (1) has short **PK**-proofs.

Theorem 3.2. *The sequent* (1) *has cut-free* **PK** *proof of size polynomial in* n.

Proof Idea. We construct a cut-free **PK** proof of (1) inductively. It will be clear from our construction that the proof has size polynomial in n.

For $n = 1$ we have:

$$\dfrac{\dfrac{p_1 \longrightarrow p_1}{p_1 \longrightarrow p_1, q_1} \qquad \dfrac{q_1 \longrightarrow q_1}{q_1 \longrightarrow p_1, q_1}}{p_1 \vee q_1 \longrightarrow p_1, q_1}$$

Now suppose that for each $i < n$ we have a proof of

$$\alpha_1 \vee \beta_1, \ldots, \alpha_i \vee \beta_i \longrightarrow p_i, q_i$$

By weakening, we can derive

$$\Gamma_{n-1} \longrightarrow p_i, q_i$$

for $i < n$, where

$$\Gamma_{n-1} = \alpha_1 \vee \beta_1, \ldots, \alpha_{n-1} \vee \beta_{n-1}$$

Then for each $i < n$, we can derive

$$(\neg p_i \wedge \neg q_i), \Gamma_{n-1} \longrightarrow$$

(by $\neg$-left, and then $\wedge$-left).

By (repeated use of) the $\vee$-left, we obtain the sequent

$$\mathcal{S} \quad = \quad \bigvee_{i=1}^{n-1} (\neg p_i \wedge \neg q_i), \Gamma_{n-1} \longrightarrow$$

Now

$$\dfrac{\dfrac{\dfrac{\mathcal{S}}{\gamma, \Gamma_{n-1} \longrightarrow p_n} \qquad p_n \longrightarrow p_n}{\alpha_n, \Gamma_{n-1} \longrightarrow p_n} \qquad \dfrac{\dfrac{\mathcal{S}}{\gamma, \Gamma_{n-1} \longrightarrow q_n} \qquad q_n \longrightarrow q_n}{\beta_n, \Gamma_{n-1} \longrightarrow q_n}}{\alpha_n \vee \beta_n, \Gamma_{n-1} \longrightarrow p_n, q_n}$$

where

$$\gamma \;=\; \bigvee_{i=1}^{n-1} (\neg p_i \wedge \neg q_i)$$

(so $\alpha_n \equiv \gamma \vee p_n$ and $\beta_n \equiv \gamma \vee q_n$). □

By the same proof, all our generalizations of the sequent (1) presented below also have polynomial-size cut-free **PK** (or, for quantified Boolean formulas, **G**)-proof.

Finally, we show that (1) also has short proofs if the cut rule is allowed for cut-formulas of depth 1. (This slightly improves the result from [CK02] which states for cut-formulas of depth 2.)

Theorem 3.3. *The sequent* (1) *have polynomial-size* 1-**PK*** *proofs.*

Proof. First we derive (by tree-like cut-free derivation):

$$p_1 \vee q_1, \ldots, p_i \vee q_i, \alpha_{i+1} \vee \beta_{i+1} \longrightarrow p_{i+1} \vee q_{i+1}$$

for $1 \leq i \leq n-1$.

From the above sequents, by repeated cuts (on $p_i \vee q_i$), we obtain

$$\alpha_1 \vee \beta_1, \ldots, \alpha_n \vee \beta_n \longrightarrow p_n \vee q_n$$

Combine this and

$$p_n \vee q_n \longrightarrow p_n, q_n$$

by a cut, we obtain (1). □

4 Separating d-PK* from Cut-Free PK

We generalize the sequent (1) by replacing each atom p_i, q_i by a formula of the form

$$\mathit{parity}(x_1^i, \ldots, x_m^i) \wedge \mathit{parity}(y_1^i, \ldots, y_m^i)$$

for some m depending on n. Here *parity* is a formula (of depth $\mathcal{O}(\log m)$ and size polynomial in m) expressing the fact that there is an odd number of 1 inputs.

In particular, let

$$\alpha_1 \equiv P_1, \quad \beta_1 \equiv Q_1$$

$$\alpha_{i+1} \equiv \left(\bigvee_{j=1}^{i} (\neg P_j \wedge \neg Q_j) \right) \vee P_{i+1}, \quad \beta_{i+1} \equiv \left(\bigvee_{j=1}^{i} (\neg P_j \wedge \neg Q_j) \right) \vee Q_{i+1}$$

where

$$P_i \equiv X_i \wedge Y_i, \quad Q_i \equiv Z_i \wedge T_i$$
$$X_i \equiv \mathit{parity}(x_1^i, \ldots, x_m^i), \quad Y_i \equiv \mathit{parity}(y_1^i, \ldots, y_m^i)$$
$$Z_i = \mathit{parity}(z_1^i, \ldots, z_m^i), \quad T_i \equiv \mathit{parity}(t_1^i, \ldots, t_m^i)$$

Theorem 4.1. *For any $d \geq 0$, for n sufficiently large, for $m \geq n^{2(d+1)}$, any d-$\mathbf{PK}^\star$ proof of the sequent*

$$(\alpha_1 \vee \beta_1), \ldots, (\alpha_n \vee \beta_n) \longrightarrow P_n, Q_n \tag{3}$$

has size $\geq 2^n$.

Note that if m is polynomial in n, then the sequent (3) has size polynomial in n. The above theorem asserts that any d-$\mathbf{PK}^\star$ proof of (3) must have size superpolynomial in the size of the sequent.

Corollary 4.2. *For any $d \geq 0$, d-$\mathbf{PK}^\star$ does not simulate cut-free* **PK**.

To prove the theorem, we use the same idea as in the proof of Theorem 3.1. Intuitively, we show that there must be branches of the proof where for each i, either a disjunction $\alpha_i \vee \beta_i$ is formed (by the $\vee$-left rule) or one of the conjunctions $X_i \wedge Y_i$ or $Z_i \wedge T_i$ is formed (using the $\wedge$-right rule). As a result, the proof size must be at least 2^n.

Consider a d-$\mathbf{PK}^\star$ proof π of (3). The idea is to follow the paths of π (starting at the root sequent (3)) until we hit a branching due to the rule $\vee$-left (where the principal formula is $\alpha_i \vee \beta_i$ for some i) or the rule $\wedge$-right (where the principal formula is $X_i \wedge Y_i$ or $Z_i \wedge T_i$, for some i). For example, consider a sequent $\mathcal{S}$ where such branching occurs:

$$\frac{\mathcal{S}_1 \qquad \mathcal{S}_2}{\mathcal{S}} = \frac{\Gamma, \alpha_i \longrightarrow \Delta \qquad \Gamma, \beta_i \longrightarrow \Delta}{\Gamma, \alpha_i \vee \beta_i \longrightarrow \Delta} \tag{4}$$

As in the proof of Theorem 3.1, we want to argue that for some such sequent $\mathcal{S}$, the subproofs of $\mathcal{S}_1$ and $\mathcal{S}_2$ are as large as the proof of (3) for $(n-1)$ pairs α_i, β_i.

The issue with a d-$\mathbf{PK}^\star$ proof is that for some $\mathcal{S}$, such $\mathcal{S}_1$, $\mathcal{S}_2$ might be trivially true (e.g., derived by the weakening rule from some tautology), and so have small proofs. The problem comes essentially from the fact that $\mathcal{S}$ may contain some other formulas of depth $\leq d$ which will be cut later.

Notation A formula A in a sequent $\mathcal{S}$ is called a *side formula* if it has depth $\leq d$.

We will show that the sequents $\mathcal{S}_1$ and $\mathcal{S}_2$ in (4) require the proof of the same size as the proof of (3) (for $(n-1)$ pairs α_i, β_i) if, intuitively, the side formulas do not contribute much to the validity of $\mathcal{S}_1$ and $\mathcal{S}_2$. This can be made precise by the following notion, which is central to our proof below.

Definition 4.3. *Suppose that $\mathcal{S}$ is a sequent of the form*

$$\Gamma', A, \ldots \longrightarrow \Delta', B, \ldots$$

where Γ' and Δ' contains all formulas of depth $\geq (d+1)$ in $\mathcal{S}$, and $A, \ldots, B, \ldots$ are all side formulas in $\mathcal{S}$. We say that a truth assignment τ is good *for $\mathcal{S}$ if it satisfies all A and falsifies all B.*

For example, if there are no side formulas in $\mathcal{S}$, then all truth assignments are good for $\mathcal{S}$. On the other hand, if $\mathcal{S}$ can be derived from the side formulas just by weakening, then it has no good assignment.

We measure the "contribution" of the side formulas to the validity of a sequent $\mathcal{S}$ by the size of the set of good assignments for $\mathcal{S}$. In particular, we will be interested in sequents with a large fraction of good assignments, i.e., sequents where the side formulas play only minor role, and thus do not help much in reducing the size of the proof of the sequents.

First, note that good truth assignments are preserved upward in the following sense:

Lemma 4.4. *Suppose that $\mathcal{S}$ is derived from $\mathcal{S}_1$ (or $\mathcal{S}_1$ and $\mathcal{S}_2$) by an inference where the principal formula has depth $\leq d$. Then a good truth assignment for $\mathcal{S}$ is also a good assignment for $\mathcal{S}_1$ (resp. a good assignment for either $\mathcal{S}_1$ or $\mathcal{S}_2$).*

4.1 Hardness of *parity*

We use the following fact about the hardness of *parity* [Has86, Has87]:

Theorem 4.5. *Any $\mathbf{AC}^0$ circuit of depth d and size $2^{m^{1/(d+1)}}$ computes the function parity$(x_1, \ldots, x_m)$ correctly on less than a $1/2 + 1/2^{m^{1/(d+1)}}$ fraction of the inputs, for sufficiently large m.*

Corollary 4.6. *Suppose that $C(x_1, \ldots, x_m)$ is a formula of size $\leq 2^{m^{1/(d+1)}}$ and depth d, and that there are at least a fraction of $2/2^{m^{1/(d+1)}}$ truth assignments that satisfy C. Then among all truth assignments that satisfy C, at least a fraction of $\frac{1}{4}$ satisfy parity$(\vec{x})$, and at least a fraction of $\frac{1}{4}$ falsify parity$(\vec{x})$.*

Proof. Let r be the fraction of truth assignments satisfy C. Then $r \geq 2/2^{m^{1/(d+1)}}$. Suppose that among the truth assignments that satisfy C, there is a fraction of s that satisfy *parity*. We show that $s \geq \frac{1}{4}$. Similar proof will show that there is a fraction of $\frac{1}{4}$ truth assignments that satisfy C falsify *parity*.

The fraction of truth assignments that satisfy $C \wedge \neg$*parity* is

$$r(1-s)$$

and the fraction of truth assignment that satisfy $\neg C \wedge$ *parity* is

$$\frac{1}{2} - rs$$

By Theorem 4.5 above, $\neg C$ computes *parity* correctly on less than a fraction of

$$\frac{1}{2} + \frac{1}{2^{m^{1/(d+1)}}} \leq \frac{1}{2} + \frac{1}{2}r$$

of all truth assignments. It follows that

$$r(1-s) + \frac{1}{2} - rs \leq \frac{1}{2} + \frac{1}{2}r$$

Hence $s \geq \frac{1}{4}$. □

We apply the above corollary in the following context.

Corollary 4.7. *Suppose that $\mathcal{S}$ is a sequent with $4km$ variables in P_i, Q_i ($1 \leq i \leq k$), where the total size of side formulas in $\mathcal{S}$ is $\leq 2^{m^{1/(d+1)}}$, and that $\mathcal{S}$ has a fraction of t good truth assignments, where $t \geq 4/2^{m^{1/(d+1)}}$. Then for each truth values v, u, there is a partial truth assignment τ_0 to the variables in P_i, Q_i so that $\tau_0(P_i) = v, \tau_0(Q_i) = u$, and the resulting sequent $\mathcal{S}|_{\tau_0}$ has at least a fraction of $t/2^5$ good assignments.*

Proof. Without loss of generality, suppose that $v = u = \top$ (True). First we find a lower bound for the number of good assignment for $\mathcal{S}$ that satisfy P_i, Q_i (i.e., that satisfy X_i, Y_i, Z_i, T_i simultaneously).

Let M denote the set of all partial truth assignments to $4(k-1)m$ variables in

$$P_1, Q_1, \ldots, P_{i-1}, Q_{i-1}, P_{i+1}, Q_{i+1}, \ldots, P_k, Q_k$$

Then

$$|M| = 2^{4(k-1)m}$$

Let

$$r = 2/2^{m^{1/(d+1)}}$$

(then $t \geq 2r$). Let $M_1 \subseteq M$ be the set of all partial truth assignments in M that can be extended to $< r2^{4m}$ good truth assignments for $\mathcal{S}$. Let the size of M_1 be

$$s2^{4(k-1)m}$$

In other words, there are $(1-s)2^{4(k-1)m}$ partial truth assignments in M that can be extended to at least $r2^{4m}$ good truth assignments for $\mathcal{S}$. An upper bound for s is obtained as follows.

The total number of good assignments for $\mathcal{S}$ is at most

$$\begin{aligned} &(1-s)2^{4(k-1)m}2^{4m} + s2^{4(k-1)m}r2^{4m} \\ =&(1-s+rs)2^{4km} \end{aligned}$$

Therefore

$$1 - s + rs \geq t$$

Hence $s \leq \frac{1-t}{1-r}$.

Now the total number of good truth assignments for $\mathcal{S}$ that are extensions of truth assignments in M_1 is at most

$$s2^{4(k-1)m}r2^{4m} \leq \frac{r-rt}{1-r}2^{4km}$$

As a result, the total number of good truth assignments for $\mathcal{S}$ that are extension of truth assignments in $M \setminus M_1$ is at least

$$(t - \frac{r-rt}{1-r})2^{4km} = \frac{t-r}{1-r}2^{4km} \geq (t-r)2^{4km} \geq \frac{t}{2}2^{4km}$$

(since $t \geq 2r$).

For each partial truth assignment $\tau \in M \setminus M_1$, by Corollary 4.6 at least a fraction of $(\frac{1}{4})^4 = \frac{1}{2^8}$ extensions of τ satisfy X_i, Y_i, Z_i, T_i simultaneously. Thus, there are at least

$$\frac{t}{2^9}2^{4km}$$

good truth assignments of $\mathcal{S}$ that satisfy P_i, Q_i simultaneously.

On the other hand, among all 2^{4m} truth assignments to the variables in P_i, Q_i, there are

$$\frac{2^{4m}}{2^4}$$

assignments that satisfies X_i, Y_i, Z_i, T_i simultaneously. As a result, there is a truth assignment τ_0 to the variables $\vec{x_i}, \vec{y_i}, \vec{z_i}, \vec{t_i}$ that satisfies X_i, Y_i, Z_i, T_i simultaneously and that can be extended to at least

$$\frac{2^4}{2^{4m}}\frac{t}{2^9}2^{4km} = \frac{t}{2^5}2^{4(k-1)m}$$

good truth assignments for S. Hence $\mathcal{S}|_{\tau_0}$ has a fraction of $t/2^5$ good truth assignments. □

Corollary 4.8. *Suppose that $\mathcal{S}$ is a sequent with $4km$ variables in P_i, Q_i ($1 \leq i \leq k$), where the total size of the side formulas in $\mathcal{S}$ is $\leq 2^{m^{1/(d+1)}}$, and that $\mathcal{S}$ has a fraction of t good truth assignments, where*

$$t \geq 2^{5(k-1)}\frac{4}{2^{m^{1/(d+1)}}} = \frac{2^{5k-3}}{2^{m^{1/(d+1)}}}$$

Then for any $2k$ truth values v_i, u_i, $1 \leq i \leq k$, there is a partial truth assignment τ to the variables in $\mathcal{S}$ so that $\tau(P_i) = v_i, \tau(Q_i) = u_i$ for $1 \leq i \leq k$.

Proof. The Corollary is proved by induction on k, using Corollary 4.7 above. □

4.2 Proof of Theorem 4.1

Theorem 4.1 follows from the theorem below by setting $k = n$:

Theorem 4.9. *Suppose that $d \geq 0$ and $m \geq n^{2(d+1)}$. Let $k \leq n$ and $\mathcal{S}$ be a sequent (involving $4km$ variables) of the form*

$$\alpha_1 \vee \beta_1, \ldots, \alpha_k \vee \beta_k, A, \ldots \longrightarrow P_k, Q_k, B, \ldots \tag{5}$$

where $A, \ldots, B, \ldots$ is the list of side formulas with total size $< 2^k$. Suppose that at least a fraction of

$$t(n,k) = \frac{1}{2^{(k+6)+\ldots+(n+5)}}$$

of all truth assignments to variables in $\mathcal{S}$ are good for $\mathcal{S}$ (here $t(n,n) = 1$). Then for n sufficiently large, any d-$\mathbf{PK}^\star$ proof of $\mathcal{S}$ must have size at least 2^k.

The remainder of this section is devoted to the proof of the above theorem.

Proof of Theorem 4.9. The proof is by induction on k.

Base case: $k = 1$. There is at most 1 side formula. The number of good truth assignments for $\mathcal{S}$ is at least

$$\frac{1}{2^{7+\ldots+(n+5)}} 2^{4m} > 1$$

(since $m \geq n^{2(d+1)}$).

So the side formula in $\mathcal{S}$, if there is any, does not constitute a tautology, and hence a proof of $\mathcal{S}$ must be obtained with an application of the $\vee$-left rule. Therefore it must have size ≥ 2.

Induction step: Suppose that the claim is true for $k-1$, for some $k \geq 2$. We prove it for k.

Let π be a proof of (5). Consider the subtree π_1 of π which is obtained by following all paths in π (starting with the root $\mathcal{S}$), until we hit one of the following:

- a $\vee$-left rule where the principal formula is some $\alpha_i \vee \beta_i$, or
- a $\wedge$-right rule where the principal formula is in $\{X_i \wedge Y_i, Z_i \wedge T_i\}$, or
- a weakening rule, where the new formula is in $\{\alpha_i \vee \beta_i, X_i \wedge Y_i, Z_i \wedge T_i\}$.

(This procedure guarantees that π_1 does not contain any leaf of π.)

Note that in π_1 all principal formulas have depth $\leq d$. By Lemma 4.4, the total number of good truth assignment for all sequents at the leaves of π_1 is at least the total number of good truth assignment for $\mathcal{S}$.

Now, if π_1 has size $\geq 2^k$, then so is π, and we are done. Otherwise, there must be leaf $\mathcal{S}'$ of π_1 where at least $1/2^k$ good assignments of $\mathcal{S}$ are also good assignments for $\mathcal{S}'$. In other words, $\mathcal{S}'$ has a fraction of at least

$$\frac{1}{2^k} t(n,k) = \frac{1}{2^k} \frac{1}{2^{(k+6)+\ldots+(n+5)}}$$

good truth assignments.

We argue that $\mathcal{S}'$ can not be obtained from some sequent $\mathcal{S}''$ by a weakening rule. For example, suppose by way of contradiction that $\mathcal{S}'$ is obtained from $\mathcal{S}''$ by weakening-left rule:

$$\frac{\mathcal{S}''}{\mathcal{S}'} = \frac{\alpha_1 \vee \beta_1, \ldots, \alpha_{i-1} \vee \beta_{i-1}, \alpha_{i+1} \vee \beta_{i+1}, \ldots, \alpha_k \vee \beta_k, A, \ldots \longrightarrow P_k, Q_k, B, \ldots}{\alpha_1 \vee \beta_1, \ldots, \alpha_k \vee \beta_k, A, \ldots \longrightarrow P_k, Q_k, B, \ldots}$$

We use Corollary 4.8 to get a contradiction. Here the fact that $m \geq n^{2(d+1)}$ ensures that

$$\frac{1}{2^{(k+6)+\ldots+(n+5)}} \geq \frac{2^{5k-3}}{2^{m^{1/(d+1)}}}$$

for sufficiently large n. By Corollary 4.8, there is a good truth assignment τ for $\mathcal{S}''$ that falsifies

$$\alpha_1 \vee \beta_1, \ldots, \alpha_{i-1} \vee \beta_{i-1}, \alpha_{i+1} \vee \beta_{i+1}, \ldots, \alpha_k \vee \beta_k, \longrightarrow P_k, Q_k$$

(Simply take a τ that satisfies $P_1, Q_1, \ldots, P_{i-1}, Q_{i-1}$ and falsifies $P_i, Q_i, \ldots, P_k, Q_k$.) Such τ falsifies $\mathcal{S}''$ (contradiction).

Now consider the case where $\mathcal{S}$ is obtained by $\vee$-left where the principal formula is $\alpha_i \vee \beta_i$. (The case where $\mathcal{S}$ is obtained by $\wedge$-right is similar.)

$$\frac{\mathcal{S}_1 \qquad \mathcal{S}_2}{\mathcal{S}'} = \frac{\Gamma, \alpha_i, A, \ldots \longrightarrow P_k, Q_k, B, \ldots \qquad \Gamma, \beta_i, A, \ldots \longrightarrow P_k, Q_k, B, \ldots}{\Gamma, \alpha_i \vee \beta_i, A, \ldots \longrightarrow P_k, Q_k, B, \ldots}$$

where

$$\Gamma = \alpha_1 \vee \beta_1, \ldots, \alpha_{i-1} \vee \beta_{i-1}, \alpha_{i+1} \vee \beta_{i+1}, \ldots, \alpha_k \vee \beta_k,$$

Here $A, \ldots, B, \ldots$ is the list of all side formulas.

First, if the total size of the side formulas in $\mathcal{S}_1$ is $\geq 2^{k-1}$, then π has size $\geq 2^k$, and we are done. So suppose that the total size of the side formulas in $\mathcal{S}_1$ is $< 2^{k-1}$.

As in the proof of Theorem 3.1, we will show that $\mathcal{S}_1$ and $\mathcal{S}_2$ require large proofs. We use the fact (as in the proof of Theorem 3.1) that under appropriate truth assignments to the variables in P_i, Q_i, a proof of $\mathcal{S}_1$ (or $\mathcal{S}_2$) can be transformed into a proof (of the same size) of (5) for $k-1$ pairs P_j, Q_j. Then by the induction hypothesis, the proofs of $\mathcal{S}_1$ and $\mathcal{S}_2$ must have size at least 2^{k-1}. As a result, π must have size at least 2^k.

Formally we consider the following cases:

Case I: $i < k$. By Corollary 4.7, there is a partial truth assignment τ_0 to the variables in X_i, Y_i, Z_i and T_i such that $\tau_0(P_i) = \tau_0(Q_i) = \top$ (True), and such that $\mathcal{S}'|_{\tau_0}$ has at least a fraction of

$$\frac{1}{2^5}\frac{1}{2^k}\frac{1}{2^{(k+6)+\ldots+(n+5)}} = \frac{1}{2^{(k+5)+\ldots+(n+5)}} = t(n, k-1)$$

good truth assignments.

Now, for $i+1 \leq j \leq k$, let

$$\alpha''_j \equiv \left(\bigvee_{\ell=1,\ldots,j-1;\ell\neq i} (\neg P_\ell \wedge \neg Q_\ell) \right) \vee P_j, \;\; \beta''_j \equiv \left(\bigvee_{\ell=1,\ldots,j-1;\ell\neq i} (\neg P_\ell \wedge \neg Q_\ell) \right) \vee Q_j$$

and let $\mathcal{S}''$ be the sequent

$$\alpha_1 \vee \beta_1, \ldots, \alpha_{i-1} \vee \beta_{i-1}, \alpha''_{i+1} \vee \beta''_{i+1}, \ldots, \alpha''_k \vee \beta''_k, A', \ldots \longrightarrow P_k, Q_k, B', \ldots$$

where $A' \equiv A|_{\tau_0}, B' \equiv B|_{\tau_0}$, etc. The sequent $\mathcal{S}''$ has the same set of good truth assignments as $\mathcal{S}'|_{\tau_0}$. So by the induction hypothesis, any d-$\mathbf{PK}^\star$ proof of $\mathcal{S}''$ has size $\geq 2^{k-1}$.

Consider the subproof π' of $\mathcal{S}_1$ in π. Then $\pi'|_{\tau_0}$ is a proof of $\mathcal{S}'_1 = \mathcal{S}_1|_{\tau_0}$. Lemma 4.10 below asserts that any proof of $\mathcal{S}'_1$ can be transformed to a proof of $\mathcal{S}''$ of smaller size. It follows that π' has size at least 2^{k-1}. The same arguments apply for the subproof of $\mathcal{S}_2$.

Case II: $i = k$. This case is handled similarly, as in the proof of Theorem 3.1. Here we need the truth assignments τ_0 where $\tau_0(P_k) = \tau_0(Q_k) = \bot$ (False). $\square$

Lemma 4.10. *Any d-$\mathbf{PK}^\star$ proof of $\mathcal{S}'_1$ (or $\mathcal{S}'_2$) can be transformed to a d-$\mathbf{PK}^\star$ proof of $\mathcal{S}''$ of smaller size.*

Proof Sketch. Note that $\mathcal{S}'_1$ has the form

$$\alpha_1 \vee \beta_1, \ldots, \alpha_{i-1} \vee \beta_{i-1}, \alpha'_i, \alpha'_{i+1} \vee \beta'_{i+1}, \ldots, \alpha'_k \vee \beta'_k, A', \ldots \longrightarrow P_k, Q_k, B', \ldots$$

where (write C for $P_i|_{\tau_0}$ and D for $Q_i|_{\tau_0}$—note that $C \Leftrightarrow \top, D \Leftrightarrow \top$):

$$\alpha'_i \equiv \left(\bigvee_{\ell=1}^{i-1} (\neg P_\ell \wedge \neg Q_\ell) \right) \vee C$$

(i.e., $\alpha'_i \Leftrightarrow \top$) and for $i < j \leq k$:

$$\alpha'_j \equiv \left(\left(\bigvee_{\ell=1}^{i-1} (\neg P_\ell \wedge \neg Q_\ell) \right) \vee (\neg C \wedge \neg D) \vee \left(\bigvee_{\ell=i+1}^{j-1} (\neg P_\ell \wedge \neg Q_\ell) \right) \right) \vee P_j$$

(Similarly for β'_i and β'_j where $i < j \leq k$.)

We use the fact that C and D are true sentences. Consider a the proof of $\mathcal{S}'_1$. The disjunction

$$\left(\bigvee_{\ell=1}^{i-1} (\neg P_\ell \wedge \neg Q_\ell) \right) \vee (\neg C \wedge \neg D)$$

must be formed by the rule $\vee$-left as follows:

$$\frac{\left(\bigvee_{\ell=1}^{i-1} (\neg P_\ell \wedge \neg Q_\ell) \right), \Gamma \longrightarrow \Delta \qquad (\neg C \wedge \neg D), \Gamma \longrightarrow \Delta}{\left(\bigvee_{\ell=1}^{i-1} (\neg P_\ell \wedge \neg Q_\ell) \right) \vee (\neg C \wedge \neg D), \Gamma \longrightarrow \Delta}$$

Modify the proof of $\mathcal{S}_1'$ by removing the subtree rooted at the upper-right sequent, as well as removing all occurrences of $(\neg C \wedge \neg D)$ from the bottom sequent and all sequents below it in the path to the root. $\square$

5 Analysis

The previous proof can be generalized as follows. Consider a proof system $\mathcal{P}$ (which might be **PK**, **PK**$[m]$, or **G**) and a class of cut formulas $\mathcal{C}$. We want to show that under some hardness assumption, tree-like $\mathcal{C}$-$\mathcal{P}$ ($\mathcal{C}$-$\mathcal{P}^\star$) does not simulate cut-free $\mathcal{P}$.

Some requirements, which are quite natural, are that $\mathcal{C}$ is closed under taking subformulas and negation, and that $\mathcal{P}$ preserves (upward) total number of good truth assignments (see Lemma 4.4). All classes $\mathcal{C}$ and proof systems $\mathcal{P}$ that we consider here satisfy these requirements.

For example, we have considered $\mathcal{C}$ to be the depth d formulas. Another example is where $\mathcal{C} = \mathbf{\Sigma}_i^q$, and $\mathcal{P} = G$; here $\mathcal{C}$-$\mathcal{P}^\star = \mathbf{G}_i^\star$.

Let $\mathit{hard}(x_1, \ldots, x_m)$ be a formula that is "hard" for formulas in $\mathcal{C}$ (see Hardness Assumption below). For $1 \leq i \leq n$, let X_i, Y_i, Z_i, T_i be as before except for using *hard* instead of *parity*:

$$X_i \equiv \mathit{hard}(x_1^i, \ldots, x_m^i), \quad Y_i \equiv \mathit{hard}(y_1^i, \ldots, y_m^i)$$
$$Z_i = \mathit{hard}(z_1^i, \ldots, z_m^i), \quad T_i \equiv \mathit{hard}(t_1^i, \ldots, t_m^i)$$

and $P_i, Q_i, \alpha_i, \beta_i$ are as in Theorem 4.1.

Theorem 5.1. *Suppose that the formula hard and set $\mathcal{C}$ satisfy the Hardness Assumption below. Then for n sufficiently large and m as in the Hardness Assumption, any $\mathcal{C}$-$\mathcal{P}^\star$ proof of the sequent*

$$(\alpha_1 \vee \beta_1), \ldots, (\alpha_n \vee \beta_n) \longrightarrow P_n, Q_n \tag{6}$$

has size $\geq 2^n$.

Corollary 5.2. *Suppose that the Hardness Assumption holds. Then $\mathcal{C}$-$\mathcal{P}^\star$ does not simulate cut-free $\mathcal{P}$.*

Our hardness assumption generalizes Theorem 4.5.

Hardness Assumption for $\mathcal{C}$: *There are a Boolean function $\mathit{hard}(x_1, \ldots, x_m)$ and a function $g(m)$ that satisfy: for each n sufficiently large, there is m so that*

- **(i)** *$g(m) \geq n^2$ and 2^n is $\omega(p(m, |\mathit{hard}(x_1, \ldots, x_m|))$ for any polynomial p, and*
- **(ii)** *any conjunction φ of the form*

$$\varphi \equiv \bigwedge_{A \in \mathcal{C}} A$$

where φ has size $< 2^n$, neither φ nor $\neg\varphi$ compute $\mathit{hard}(x_1, \ldots, x_m)$ correctly on more than a fraction of $h + 1/2^{g(m)}$ inputs.

Here $h \geq 1/2$ is the fraction of inputs that satisfy hard.

The assumption holds for *hard* = *parity* and $\mathcal{C}$ is the class of depth d formulas: Theorem 4.5 shows that we can take $g(m) = m^{1/(d+1)}$ (there $h = 1/2$).

Theorem 5.1 follows from the next Theorem (cf. Theorem 4.9):

Theorem 5.3. *Suppose that the Hardness Assumption holds for hard and $\mathcal{C}$. Let n be sufficiently large, and m be as in the Hardness Assumption. Let $\mathcal{S}$ be a sequent of the form*

$$\alpha_1 \vee \beta_1, \ldots, \alpha_k \vee \beta_k, A, \ldots \longrightarrow P_k, Q_k, B, \ldots$$

where $A, \ldots, B, \ldots$ is the list of side formulas with total size $< 2^k$. Suppose that at least a fraction of

$$t(n,k) = \frac{1}{2^{(k+6)+\ldots+(n+5)}}$$

of all truth assignments to variables in $\mathcal{S}$ are good for $\mathcal{S}$ (here $t(n,n) = 1$). Then any $\mathcal{C}$-$\mathcal{P}^\star$ proof of $\mathcal{S}$ must have size at least 2^k.

Proof. We proceed just as in the proof of Theorem 4.9. Here we use $g(m)$ for $m^{1/(d+1)}$. Analogues of Corollaries 4.6–4.8 can be proved for the formulas in $\mathcal{C}$ from the Hardness Assumption. □

6 Applications

In this section we apply the general analysis from the previous section to obtain some new (possibly conditional) separations. This section is organized as follows. First, in Subsection 6.1 we show that d-$\mathbf{PK}^\star$ does not simulate cut-free **PK** for sequents of some constant depth (the constant depends on d). (The separating sequents in Section 4 have logarithmic depth.) Then in Subsection 6.2 we consider the sequent calculus **G** for quantified Boolean formulas. Finally, we formally define $\mathbf{PK}[p]$ and show (unconditionally) that d-$\mathbf{PK}^\star$ does not simulate 5-$\mathbf{PK}^\star[p]$ for sequents of constant depth (depending on d).

6.1 Hard, Small Depth Sequents for d-$\mathbf{PK}^\star$

Corollary 6.1. *Tree-like d-**PK** does not simulate cut-free **PK** for sequents of depth $2d + 8$.*

As we mentioned in the introduction, d-$\mathbf{PK}^\star$ p-simulates $(d-1)$-**PK** for sequents of depth $(d-1)$. So the above Corollary give an upper bound on the depth of sequents on which d-$\mathbf{PK}^\star$ simulates $(d-1)$-**PK**.

We use the following fact:

Lemma 6.2. *For each $d \geq 2$, there is a $\vee$-$\wedge$ formula parity_d of depth d, size $m2^{(d-1)m^{1/(d-1)}}$ that computes $\text{parity}(x_1, \ldots, x_m)$.*

Proof. We prove by induction on $d \geq 2$ that there are $\vee$-$\wedge$ formula parity_d and $\wedge$-$\vee$ formula parity'_d of size $m2^{(d-1)m^{1/(d-1)}}$ and depth d that computes *parity*.

For the base case, we can take the obvious DNF and CNF formulas (of size $< m2^m$).

For the induction step, we show how to obtain the $\vee$-$\wedge$ formula parity_d. The $\wedge$-$\vee$ formula parity'_d is obtained from parity'_d by interchanging $\vee$ and $\wedge$, and interchanging the literals x_i and $\neg x_i$ for all but one i.

First, note that

$$\neg \mathit{parity}_{d-1}(\vec{x}) \Leftrightarrow \overline{\mathit{parity}}_{d-1}(\vec{x}) \Leftrightarrow \overline{\mathit{parity}}'_{d-1}(\vec{x})$$

where $\overline{\mathit{parity}}_{d-1}(\vec{x})$ is the $\vee$-$\wedge$ formula obtained from $\mathit{parity}_{d-1}(\vec{x})$ by interchanging x_1 and $\neg x_1$, and similarly for $\overline{\mathit{parity}}'_{d-1}(\vec{x})$.

Divide the inputs into $k = m^{1/(d-1)}$ blocks of size $m^{(d-2)/(d-1)}$. Now parity_d is the disjunction of 2^{k-1} formulas of the form

$$B_1 \wedge \ldots \wedge B_k$$

where B_i is either $\mathit{parity}'_{d-1}(x_{ik}, \ldots, x_{(i+1)k-1})$ or $\overline{\mathit{parity}}'_{d-1}(x_{ik}, \ldots, x_{(i+1)k-1})$. Note that all B_i are $\wedge$-$\vee$ formulas.

There are $k2^{k-1}$ occurrences of the B_i and $(2^{k-1}+1)$ new connectives. By the induction hypothesis, each B_i has size at most $m^{(d-2)/(d-1)}2^{(d-2)m^{1/(d-1)}}$. Therefore the size of parity'_d is at most

$$k2^{k-1}m^{(d-2)/(d-1)}2^{(d-2)m^{1/(d-1)}} + (2^{k-1}+1) < m2^{(d-1)m^{1/(d-1)}}$$

(since $k = m^{1/(d-1)}$). □

Proof of Corollaries 6.1. To prove the lower bound for d-$\mathbf{PK}^\star$, we use the formula parity_{2d+4} from Lemma 6.2 in place of *hard*. Note that now the sequent (6) has depth $2d+8$.

The Hardness Assumption holds for the class of depth d formulas and parity_d.

The sequent (6) now has size polynomial in

$$m2^{(2d+3)m^{1/(2d+3)}}$$

Take $m = n^{2d+2}$, then Theorem 5.1 shows that any d-$\mathbf{PK}^\star$ proof of (6) must have size 2^n, which is superpolynomial in the size of (6).

The upper bound for cut-free **PK** and $(2d+5)$-$\mathbf{PK}^\star$ are proved just as for Statman's original sequents. □

We can reduce the depth of the sequents used in the above proof to $(2d+7)$ by using appropriate formulas parity_d or parity'_d for X_i, etc., and appropriate formulas $\overline{\mathit{parity}}_d$ or $\overline{\mathit{parity}}'_d$ for $\neg X_i$, etc., in the sequent (6). We will also need the fact that the sequents

$$\mathit{parity}_d(\vec{x}) \longrightarrow \mathit{parity}'_d(\vec{x}); \qquad \mathit{parity}_d(\vec{x}), \overline{\mathit{parity}}_d(\vec{x}) \longrightarrow \ ; \qquad \text{etc.}$$

have polynomial-size cut-free $\mathbf{PK}^\star$ proofs. Details are left to the reader.

We also obtain the following separation, although it is weaker than the separation in [BB05].

Corollary 6.3. *d-$\mathbf{PK}^\star$ does not simulate $(2d+5)$-$\mathbf{PK}^\star$.*

6.2 Conditional Hard Sequents for Tree-Like $\mathbf{G}_j$

We now consider the system $\mathbf{G}$ [KP90, CM05] which is an extension of $\mathbf{PK}$ for quantified Boolean formulas. The formulas are defined inductively as before, with the addition of quantifiers $\exists, \forall$, where

$$\exists x A(x) \Leftrightarrow A(\bot) \vee A(\top), \qquad \forall x A(x) \Leftrightarrow A(\bot) \wedge A(\top)$$

$\mathbf{\Sigma}_i^q$ (resp. $\mathbf{\Pi}_i^q$) is the set of formulas that have a prenex form where there are at most i alternations of quantifiers, with the outermost quantifier being $\exists$ (resp. $\forall$).

There are four new introduction rules in $\mathbf{G}$ for the quantifiers:

$$\frac{A(B), \Gamma \longrightarrow \Delta}{\forall x A(x), \Gamma \longrightarrow \Delta}\,\forall\textbf{-left} \qquad \frac{\Gamma \longrightarrow \Delta, A(p)}{\Gamma \longrightarrow \Delta, \forall x A(x)}\,\forall\textbf{-right}$$

$$\frac{A(p), \Gamma \longrightarrow \Delta}{\exists x A(x), \Gamma \longrightarrow \Delta}\,\exists\textbf{-left} \qquad \frac{\Gamma \longrightarrow \Delta, A(B)}{\Gamma \longrightarrow \Delta, \exists x A(x)}\,\exists\textbf{-right}$$

Restriction In the rules $\forall$-**right** and $\exists$-**left**, p must not occur in the bottom sequent.

For $i \geq 0$, $\mathbf{G}_i$ is the subsystem of $\mathbf{G}$ in which all cut formulas belong to $\mathbf{\Sigma}_i^q \cup \mathbf{\Pi}_i^q$. $\mathbf{G}_i^\star$ denotes tree-like $\mathbf{G}_i$.

It is known that $\mathbf{G}_{i+1}^\star$ and $\mathbf{G}_i$ are p-equivalent for $\mathbf{\Sigma}_i^q \cup \mathbf{\Pi}_i^q$ formulas, and Perron [Per07] shows that $\mathbf{G}_i$ p-simulates $\mathbf{G}_{i+1}^\star$ for all quantified formulas.

Let $j \geq 0$. Consider the Hardness Assumption where $\mathcal{C} = \mathbf{\Sigma}_j^q$. This assumption is weaker than the (i,j)-QBF Hardness Conjecture [MP06] in that it does not require that $hard_j \in \mathbf{\Sigma}_i^q$ for any i.

Hardness Assumption for $\mathbf{\Sigma}_j^q$: *There are a quantified boolean formula*

$$hard_j(x_1, \ldots, x_m)$$

and a function $g(m)$ that satisfy: for all n sufficiently large, there is m so that **(i)** *$g(m) \geq n^2$ and 2^n is superpolynomial in $(m, |hard(x_1, \ldots, x_m|)$, and* **(ii)** *no $\mathbf{\Sigma}_j^q$ formula φ of size $< 2^n$ computes $hard(x_1, \ldots, x_m)$ correctly on more than a fraction of $h + 1/2^{g(m)}$ inputs. Here $h \geq 1/2$ is the fraction of inputs that satisfy hard.*

Corollary 6.4. *Suppose that the Hardness Assumption for $\mathbf{\Sigma}_j^q$ holds. Then $\mathbf{G}_j^\star$ does not simulate cut-free $\mathbf{G}$.*

It is known that $\mathbf{G}_0^\star$ p-simulates $\mathbf{G}_0$ for $\mathbf{\Sigma}_1^q$ formulas *in prenex form* [Mor05]. It is still consistent with our knowledge that the formula $hard_0$ (the hard formula for quantifier-free formulas) belongs to $\mathbf{\Sigma}_1^q$. This is because the formulas in our separating sequent are not in prenex form (although they are in $\mathbf{\Sigma}_1^q$).

We can also obtain a conditional separation of $\mathbf{G}_i^\star$ and $\mathbf{G}_j^\star$ where $j < i$. Here the separating sequents have polynomial-size proofs in $\mathbf{G}_i^\star$ but require superpolynomial-size proofs in $\mathbf{G}_j^\star$. (The separating sequents in [MP06] have *superpolynomial*-size proofs in both $\mathbf{G}_i^\star$ and $\mathbf{G}_j^\star$.)

Corollary 6.5. *Suppose that the Hardness Assumption for $\mathbf{\Sigma}_j^q$ holds for some formula $hard_j \in \mathbf{\Sigma}_i^q$. Then $\mathbf{G}_j^\star$ does not simulate $\mathbf{G}_i^\star$.*

Proof. Notice that if $hard_j \in \mathbf{\Sigma}_i^q$, then all formulas in the sequent (6) belong to $\mathbf{\Sigma}_i^q \cup \mathbf{\Pi}_i^q$. The proof of Theorem 3.3 can be modified to show that (6) have short proof in $\mathbf{G}_i^\star$. □

6.3 PK with Modular Counting Connectives

For $p \geq 2$, consider propositional formulas with connectives M_p^k, where

$$\mathsf{M}_p^k(x_1, \ldots, x_m) \;\Leftrightarrow\; (\text{the \# of } \top \text{ in } \vec{x} \text{ is } (k \mod p))$$

$\mathbf{PK}[p]$ is the extension of $\mathbf{PK}$ where there are additional axioms and introduction rules for the new connectives. Our definition of $\mathbf{PK}[p]$ here follows [BIK+96].

The new axioms are (in the following, mathematical operations on the superscript are taken in the group $\mathbb{Z}/p\mathbb{Z}$):

$$\longrightarrow \mathsf{M}_p^0(), \qquad \mathsf{M}_p^k() \longrightarrow \quad \text{for } 1 \leq k < p$$

and

$$\mathsf{M}_p^k(A_1, \ldots, A_n), \mathsf{M}_p^r(B_1, \ldots, B_m) \longrightarrow \mathsf{M}_p^{k+r}(A_1, \ldots, A_n, B_1, \ldots, B_m) \qquad (7)$$

$$\mathsf{M}_p^k(A_1, \ldots, A_n, B_1, \ldots, B_m), \mathsf{M}_p^r(A_1, \ldots, A_n) \longrightarrow \mathsf{M}_p^{k-r}(B_1, \ldots, B_m) \qquad (8)$$

(for $0 \leq k, r < p$).

The new rules are

$$\mathsf{M}_p^k\text{-left:}\frac{\mathsf{M}_p^k(A_2, \ldots, A_n), \Lambda \longrightarrow \Gamma \qquad A_1, \mathsf{M}_p^{k-1}(A_2, \ldots, A_n), \Lambda \longrightarrow \Gamma}{\mathsf{M}_p^k(A_1, \ldots, A_n), \Lambda \longrightarrow \Gamma}$$

$$\mathsf{M}_p^k\text{-right:}\frac{\Lambda \longrightarrow A_1, \mathsf{M}_p^k(A_2, \ldots, A_n), \Gamma \qquad \Lambda \longrightarrow \mathsf{M}_p^{k-1}(A_2, \ldots, A_n), \Gamma}{\Lambda \longrightarrow \mathsf{M}_p^k(A_1, \ldots, A_n), \Gamma}$$

Notice that the axioms (7), (8) might not be present in some existing definitions of systems with the modular counting connectives. Let *weak*$\mathbf{PK}[p]$ denote $\mathbf{PK}[p]$ without these axioms. Then *weak*$\mathbf{PK}[p]$ and $\mathbf{PK}[p]$ are polynomially

equivalent. However, it can be shown that the axioms (7), (8) require exponential *weak*$\mathbf{PK}^\star[p]$ proofs. Here, these axioms can be used to show that the sequent

$$\mathsf{M}_p^1(x_1,\ldots,x_m) \longrightarrow mod_p(x_1,\ldots,x_m)$$

has polynomial-size 1-$\mathbf{PK}^\star[p]$ proofs, where $mod_p(\vec{x})$ is a Boolean formula (of logarithmic depth, polynomial size) equivalent to $\mathsf{M}_p^1(\vec{x})$ (see (9) below).

Theorem 6.6. *Let p be a prime number, and $d \geq 0$. Then d-$\mathbf{PK}^\star$ does not simulate 5-$\mathbf{PK}^\star[p]$: There are sequents (without M_p connectives) of depth $(2d+8)$ that have polynomial-size 5-$\mathbf{PK}^\star[p]$ proofs but require superpolynomial-size d-$\mathbf{PK}^\star$ proofs.*

Note that 5-$\mathbf{PK}^\star[p]$ is stronger than 5-*weak*$\mathbf{PK}^\star[p]$. Also, this theorem does not imply the separation of *weak*$\mathbf{PK}^\star[p]$ from d-$\mathbf{PK}^\star$.

The fact that d-$\mathbf{PK}^\star$ does not simulate 5-$\mathbf{PK}^\star[p]$ can be proved using the Boolean formula $mod_p(x_1,\ldots,x_m)$ (of size polynomial in m and depth logarithmic in m) where

$$mod_p(x_1,\ldots,x_m) \Leftrightarrow \mathsf{M}_p^1(x_1,\ldots,x_m) \tag{9}$$

To prove the theorem (where the separating sequents have depth $(2d+8)$), we need the following fact:

Lemma 6.7. *For each $d \geq 2$, for $0 \leq k < p$, there is a $\vee$-$\wedge$ formula $mod_{p,k}^d$ of depth d, size $mp^{(d-1)(1+m^{1/(d-1)})}$ that computes $\mathsf{M}_p^k(x_1,\ldots,x_m)$.*

Proof. The proof is similar to the proof of Lemma 6.2. Here we prove by induction on $d \geq 2$ that for each $0 \leq i < p$, there are $\vee$-$\wedge$ formula $mod_{p,i}^{d,\vee}(x_1,\ldots,x_m)$ and $\wedge$-$\vee$ formula $mod_{p,i}^{d,\wedge}(x_1,\ldots,x_m)$ both of depth d and size $mp^{(d-1)(1+m^{1/(d-1)})}$ that compute $\mathsf{M}_p^i(x_1,\ldots,x_m)$.

For the base case, the formula $mod_{p,i}^{2,\vee}(\vec{x})$ is the obvious DNF formula of size $< mp^m$. The formula $mod_{p,i}^{2,\wedge}(\vec{x})$ is equivalent to

$$\neg \bigvee_{j \neq i} mod_{p,j}^{2,\vee}$$

The above formula can be turn into a CNF formula of the same size. Thus $mod_{p,i}^{2,\wedge}(\vec{x})$ has size $< mp^{1+m}$.

For the induction step, divide the inputs into $k = m^{1/(d-1)}$ blocks, each of size $m^{(d-2)/(d-1)}$. The formula $mod_{p,i}^{d,\vee}(x_1,\ldots,x_m)$ is the disjunction of p^k formulas of the form

$$B_1 \wedge \ldots \wedge B_k$$

where each B_ℓ is of the form $mod_{p,j}^{d-1,\wedge}(x_{\ell k},\ldots,x_{(\ell+1)k-1})$ for some j, $0 \leq j < p$.

There are kp^k occurrences of B_ℓ, each of size $< m^{(d-2)/(d-1)}p^{(d-2)(1+m^{1/(d-1)})}$, and (kp^k+1) new connectives. As a result, the size of $mod_{p,i}^{d,\vee}(x_1,\ldots,x_m)$ is at most

$$kp^k m^{(d-2)/(d-1)} p^{(d-2)(1+m^{1/(d-1)})} + (kp^k+1)$$

Hence (recall that $k = m^{1/(d-1)}$)

$$|mod_{p,i}^{d,\vee}(x_1, \ldots, x_m)| < mp^{(d-1)(1+m^{1/(d-1)})}$$

Next, the formula $mod_{p,i}^{d,\wedge}(x_1, \ldots, x_m)$ is the $\wedge$-$\vee$ equivalence of

$$\neg \bigvee_{j \neq i} mod_{p,j}^{d,\vee}(x_1, \ldots, x_m)$$

So $mod_{p,i}^{d,\wedge}(x_1, \ldots, x_m)$ has size at most

$$(p-1)\left(kp^k m^{(d-2)/(d-1)} p^{(d-2)(1+m^{1/(d-1)})} + (kp^k + 1)\right) + 1$$
$$< mp^{(d-1)(1+m^{1/(d-1)})}$$

□

Lemma 6.8. *The following sequents have polynomial-size cut-free* $\mathbf{PK}^\star[p]$ *proofs:*

$$\mathsf{M}_p^k(x_1, \ldots, x_m) \longrightarrow mod_{p,k}^d(x_1, \ldots, x_m)$$
$$mod_{p,k}^d(x_1, \ldots, x_m) \longrightarrow \mathsf{M}_p^k(x_1, \ldots, x_m)$$

Proof. The proof is by induction on d. □

Proof of Theorem 6.6. Here we use $mod_{p,1}^{2d+4}(x_1, \ldots, x_m)$ as a hard function for depth d formulas of **PK**. Note that Theorem 4.5 also applies for mod_p (hence for $mod_{p,1}^{2d+4}$).

First, let $\mathcal{S}(mod)$ be the sequent obtained from (6) by replacing *hard* by $mod_{p,1}^{2d+4}$. As before, it follows that $\mathcal{S}(mod)$ requires superpolynomial-size d-$\mathbf{PK}^\star$ proofs.

Now let $\mathcal{S}(\mathsf{M})$ be the sequent obtained from (6) by replacing $hard(x_1, \ldots, x_m)$ by $\mathsf{M}_p^1(x_1, \ldots, x_m)$. Notice that $\mathcal{S}(\mathsf{M})$ has polynomial-size 5-$\mathbf{PK}^\star[p]$ proof. (See the proof of Theorem 3.3.)

Next, we show that $\mathcal{S}(mod)$ can be derived from $\mathcal{S}(\mathsf{M})$ in 5-$\mathbf{PK}^\star[p]$ by a polynomial-size proof. Notice that from Lemma 6.8 we can derive

$$\alpha_i(mod) \vee \beta_i(mod) \longrightarrow \alpha_i(\mathsf{M}) \vee \beta_i(\mathsf{M})$$

and

$$P_n(\mathsf{M}) \longrightarrow P_n(mod), \qquad Q_n(\mathsf{M}) \longrightarrow Q_n(mod)$$

(Here $\alpha_i(mod)$, $P_n(\mathsf{M})$, etc., are the α_i, P_n in $\mathcal{S}(mod)$, $\mathcal{S}(\mathsf{M})$, respectively.)

Then by using the cut rule (with cut formulas $\alpha_i(mod) \vee \beta_i(mod)$ and $P_n(\mathsf{M})$, $Q_n(\mathsf{M})$) we obtain $\mathcal{S}(mod)$. The above cut formulas have depth 5. □

Again, note that by replacing $\neg\mathsf{M}_p^1(\vec{x})$ by

$$\bigvee_{0 \leq k < p, k \neq 1} \mathsf{M}_p^k(\vec{x})$$

we can reduce the depth of cut-formulas in the proofs above to 4. Thus d-$\mathbf{PK}^\star$ does not simulate 4-$\mathbf{PK}^\star[p]$. Details are left to the reader.

7 Conclusion

Under the Hardness Assumption for depth d formulas with the M_m^k connectives, where the hard function is MAJORITY, it can be shown that d-$\mathbf{PK}^\star[m]$ does not simulate cut-free **PK** as well as tree-like 5-$\mathbf{PTK}'$. Here $\mathbf{PTK}'$ [BC96] is the extension of **PK** for propositional logic with threshold connectives.

Under a somewhat less plausible Hardness Assumption for the same class of formulas, where the hard function can be computed by polynomial-size formulas using M_p^k connectives, then d-$\mathbf{PK}^\star[m]$ does not simulate cut-free **PK** as well as 5-$\mathbf{PK}^\star[p]$.

It is interesting to come up with a plausible candidate hard function for $\mathbf{\Sigma}_0^q$ formulas. Note that here the complexity of $hard_0(x_1, \ldots, x_m)$ may vary with m.

Overall, our results suggest that tree-like proof systems might be "fooled" by some trivially true (i.e. having short cut-free dag-like proofs) tautologies. A more difficult task is to investigate whether lower bound for dag-like proof systems can be obtained from complexity theory hardness assumptions.

Acknowledgments: This work is inspired by Toni Pitassi recent talks on [MP06]. I would like to thank Alasdair Urquhart for pointing out Statman's Theorems and many references. Thanks also to Steve Cook for helpful comments, Toni Pitassi for the conversations as well as having read a draft of this paper, and the referees for helpful feedback.

References

[Ara96] Noriko Arai. A Proper Hierarchy of Propositional Sequent Calculi. *Theorectical Computer Science*, 159:343–354, 1996.

[BB05] Arnold Beckmann and Samuel Buss. Separation Results for the Size of Constant-Depth Propositional Proofs. *Annals of Pure and Applied Logic*, 136:30–55, 2005.

[BC96] Samuel Buss and Peter Clote. Cutting Planes, Connectivity and Threshold Logic. *Archive for Mathematical Logic*, 35:33–62, 1996.

[BIK+96] Paul Beame, Russell Impagliazzo, Jan Krajíček, Toniann Pitassi, and Pavel Pudlák. Lower Bounds on Hilbert's Nullstellensatz and Propositional Proofs. *Proceedings of the London Mathematical Society*, 73:1–26, 1996.

[Bus88] Sam Buss. Weak Formal Systems and Connections to Computational Complexity. Lecture Notes for a Topic Course. University California, Berkeley, 1988.

[CK02] Peter Clote and Evangelos Kranakis. *Boolean Functions and Computation Models*. Springer, 2002.

[CM05] Stephen Cook and Tsuyoshi Morioka. Quantified Propositional Calculus and a Second-Order Theory for NC^1. *Archive for Mathematical Logic*, 44:711–749, 2005.

[CN06] Stephen Cook and Phuong Nguyen. Foundations of Proof Complexity: Bounded Arithmetic and Propositional Translations. Book in progress, 2006.

[Has86] Johan Hastad. Almost Optimal Lower Bounds for Small Depth Circuits. In *18th Annual ACM Symposium on Theory of Computing*, pages 6–20, 1986.

[Has87] Johan Hastad. *Computational limitations for small depth circuits*. MIT Press, 1987.

[KP90] Jan Krajíček and Pave Pudlák. Quantified Propositional Calculi and Fragments of Bounded Arithmetic. *Zeitschrift f. Mathematickal Logik u. Grundlagen d. Mathematik*, 36:29–46, 1990.

[Kra94] J. Krajíček. Lower bounds to the size of constant-depth propositional proofs. *J. Symbolic Logic*, 59:73–86, 1994.

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*. Cambridge University Press, 1995.

[Mor05] Tsuyoshi Morioka. *Logical Approaches to the Complexity of Search Problems: Proof Complexity, Quantified Propositional Calculus, and Bounded Arithmetic*. PhD thesis, University of Toronto, 2005.

[MP06] Alexis Maciel and Toniann Pitassi. A conditional lower bound for a system of constant-depth proofs with modular connectives. In *Proc. 21st IEEE Symposium on Logic in Computer Science*, 2006.

[Per07] Steven Perron. Examining the Fragments of G. In *Proc. 22nd IEEE Symposium on Logic in Computer Science*, 2007.

[Sta78] Richard Statman. Bounds for Proof-Search and Speed-up in the Predicate Calculus. *Annals of Mathematical Logic*, 15:225–287, 1978.