Structure of proofs and the complexity of cut elimination

Wenhui Zhang

Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, P.O. Box 8718, Beijing 100080, China

Received 31 March 2003; received in revised form 23 June 2005; accepted 21 July 2005

Communicated by J. Tiuryn

Abstract

The importance of the structure of cut-formulas with respect to proof length and proof depth has been studied in various occasions. It has been illustrated that a quantifier may be more powerful than a binary connective in cut-formulas with respect to the reduction (or increase) of proof length and proof depth, and a sequence of quantifiers of the same type (existential or universal) may be less powerful than a sequence of quantifiers of alternating types. This paper provides a refined view on cut-elimination through an analysis of the structure of proofs, brings new insight into the relation between cut-formulas and short proofs, and illustrates that a mixture of quantifiers and binary connectives could be important for achieving the maximal benefit of cut-formulas for obtaining short proofs.

© 2005 Elsevier B.V. All rights reserved.

Keywords: Proof complexity; Proof structure; Balanced proofs; Cut elimination

1. Introduction

Since the Gentzen’s cut-elimination result, cut-elimination has been a central issue of proof theory. Studying of cut-elimination in a proof system may be related to the understanding of whether proofs in such a system have properties including consistency, sub-formula property and witness property. Cut-elimination related to different languages, logics and rewrite systems has therefore been intensively studied, e.g. in [11,17,16,10,9,8]. Issues concerned in the study of cut-elimination include confluence, strong normalization, semantics and proof length. Our focus is proof length. The importance of cut-formulas with respect to proof length and proof depth has been studied in various occasions [18,19,4,20,21]. A cut-elimination theorem and general upper bounds for cut-elimination can be found in [18]. The importance of cut-formulas with respect to proof length has been studied in [19] and has been further illustrated in [4]. The importance of the structure of cut-formulas has been studied in [20,21]. From these studies, we know that given a proof of depth $n$ with cut-formulas of complexity $k$, there is a corresponding cut-free proof of depth $\leq 2^n_k$ (defined by $2^0_n = n$, $2^{i+1}_n = 2^{2^n_i}$). Different definitions of the complexity of cut-formulas reflect different or refined views on the structure of cut-formulas with respect to cut-elimination [18,20,21]. It has been illustrated that a quantifier may be more powerful than a binary connective in cut-formulas with respect to the reduction (or increase) of proof length and proof depth [20], and

$\star$ Supported by the National Natural Science Foundation of China under Grant Nos. 60223005, 60373050, 60421001 and 60573012, and the National Grand Fundamental Research 973 Program of China under Grant No. 2002cb312200.

E-mail address: zwh@ios.ac.cn.

0304-3975/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
a sequence of quantifiers of the same type (existential or universal) may be less powerful than a sequence of quantifiers of alternating types [21]. Although the complexity of cut-formulas has been defined differently in different studies, the upper bound $2^k_n$ (with a different $k$ according to their respective definitions) is roughly the same. We further study cut-formulas and cut-elimination strategies through an analysis of the structure of proofs (i.e., balanced or unbalanced proofs). As a consequence, the upper bound $2^k_n$ is reduced to roughly $2^{n/2}_k$. The analysis also illustrates that a mixture of quantifiers and binary connectives could be important for achieving the maximal benefit of cut-formulas for obtaining short proofs. This point is to be further discussed at the end of this paper.

Different systems give rise to the development of different cut-elimination strategies. For instance, Danos, Joinet and Schellinx have recently developed a proof system denoted LK¹⁹ which is a system with additional information that can be used to restrict the cut-elimination process in order to ensure a confluent and Noetherian normalization of proofs. The basic idea is to add colors to formulas and orientation to connectives or rules such that cut-elimination steps can be performed according to these additional information [7]. Carbone related proofs to logical flow graphs and developed a combinatorial model to study the evolution of graphs underlying proofs during the process of cut-elimination. Differences in the behavior of cut-elimination is explained by the differences in their two-dimensional graph structures and exponential and multi-exponential speed-ups in the number of lines of proofs are illustrated by analyzing bridge groups associated to proofs [5,6]. The main focus of our work is further investigation of the proof length, not on lower bounds related to speed-up through illustrations, rather, on upper bounds of speed-up through cut-elimination, and the starting point of our work is the Gentzen’s sequent calculus (LK), however, we shall only use a simplified version of sequent calculus for our purpose. The basic cut-elimination principle in this paper is the same as that of Gentzen’s cross-cut for moving the application of the cut-rule upwards in the proof-tree, copying parts of the proof-tree when necessary and reducing the cut-formula at the node it is composed or eliminating the use of cut at the leaf node when application of the cut-rule has been carried up to the leaf node. Similar idea is also used in Danos, Joinet and Schellinx’s tq-protocol in which there are two steps, one to move a cut-formula up in the proof-tree as far as possible and eliminate it directly when possible, and the other to reduce the cut-formula. The former step of the protocol combines some basic cut-elimination steps to form a composed step in order to partly guarantee the confluence of cut-elimination in which much of freedom of choosing cut-elimination steps still remains. We do not explicitly distinguish different steps or emphasize on the freedom of choosing cut-elimination steps, since the purpose is to eliminate or reduce a cut-formula as quickly as possible. Even so, there are still some freedom of choosing composed cut-elimination steps. A natural composed step in our analysis will be one that looks at a cut-formula and eliminates or reduces the cut-formula in a sequence of consecutive actions. Regarding the cut-elimination steps in this paper, one advantage is that the copied subproofs to be carried up in the proof-tree could be smaller in the process of cut-elimination, such that the process could be shorter comparing to cut-elimination using the original cut-elimination steps. For instance, in the original Gentzen’s cross-cut, a step may move cut-formulas of the form $\varphi \land \psi$ upwards the proof tree, while by our strategy, we copy subformulas of $\varphi \land \psi$ to relevant parts of the proof tree; cut-formulas of the form $\forall x.\varphi(x)$ are dealt with similarly such that subformulas of $\forall x.\varphi(x)$ are copied to relevant parts of the proof tree instead of moving $\forall x.\varphi(x)$ upwards the proof tree. The strategy presented in this paper involves clustering related logical connectives together and defining the set of maximal non-positive subformulas of positive formulas, similar to the focalization property discovered by Andreoli [3,1,2]. As explained by Girard in [13], the negative connectives are invertible while the positive connectives are not. An interesting property is that operations of the same polarity can be clustered together as a single operation, so that one can talk about the maximal subformulas of the opposite polarity instead of the intermediate subformulas and one can also make restrictions on occurrences of positive (or dually negative) formulas in a sequent. This property is used in polarized systems such as Girard’s Ludics [12,13] and Laurent’s Polarized Linear Logic [14,15] which introduces the use of polarized formulas into Linear Logic [11] with one sided sequents.

We also relate polarities to formulas and use one sided sequents. The simplified version of Gentzen’s sequent-calculus we are using is the one for negation normal form formulas. For the first, we only consider succedents of sequents (every sequent with antecedent and succedent is transformed into a sequent with only a succedent, if necessary); for the second, we only consider negation normal form formulas (every formula is transformed into the corresponding formula in negation normal form, if necessary); for the third, we use sets of formulas instead of lists of formulas. The purpose of this simplification is to minimize the rules in the proof system in order to concentrate on the effect of the essential cut-elimination steps with respect to our analysis. The disadvantage of this is loss of the structure of the sequent and that of the corresponding proof-tree. On the other hand, we gain the simplicity, for instance, it would be simpler to relate
polarities to connectives and formulas, because we do not need to distinguish formulas in different parts (antecedents or succedents) of sequents.

1.1. Preliminaries

A first order formula is in negation normal form if the formula is built up with predicate symbols, function symbols (including constants), first order variables, quantifiers $\forall$ and $\exists$, binary connectives $\land$ (conjunction), $\lor$ (disjunction) and unary connective $\neg$ (negation) where $\neg$ applies only to atomic formulas. Disjunction and the existential quantifier are called positive connectives. There are six types of formulas: atomic formulas, negation of atomic formulas, conjunctive formulas, disjunctive formulas, universally quantified formulas and existentially quantified formulas. Atomic formulas and negation of these are called literals. Disjunctive and existentially quantified formulas are called positive formulas.

Let $A$, $B$ denote literals, $\varphi$, $\psi$ formulas, and $A$, $\Gamma$ sets of formulas. For convenience, we write $A, \varphi$ for $A \cup \{\varphi\}$. The influence rules of the proof system are as follows:

- **Axiom:** If $\neg A \in A$, then $A$, $A$ is valid;
- **Left-disjunction:** If $A, \varphi$ is valid, then $A, \varphi \lor \psi$ is valid;
- **Right-disjunction:** If $A, \psi$ is valid, then $A, \varphi \lor \psi$ is valid;
- **Conjunction:** If $A, \varphi$ and $A, \psi$ are valid, then $A, \varphi \land \psi$ is valid;
- **Existentiality:** If $A, \varphi(x)$ is valid, then $A, \exists x. \varphi(x)$ is valid;
- **Cut:** If $A, \varphi$ and $A, \neg \varphi$ are valid, then $A$, $A$ is valid.

The rules for disjunction and existentiality are called positive rules. The formulas $\varphi \land \psi$, $\varphi \lor \psi$, $\exists x. \varphi(x)$, $\forall x. \varphi(x)$ are called the principal formula of their respective influence rules. $\varphi$ and $\neg \varphi$ in the cut-rule are called cut-formulas. Since we are dealing with negation normal form formulas, $\neg \varphi$ represents the corresponding negation normal form formula equivalent to the negation of $\varphi$. The length of a proof is the size of the proof-tree. The depth of a proof is the length of the longest branch of the proof-tree. Let $\delta$ be a proof-tree, the length and the depth of $\delta$ are denoted by $|\delta|$ and $|\delta|$, respectively. A complexity class $K$ of formulas is a set of formulas satisfying the following properties: (i) if $\varphi \in K$, then $\neg \varphi \in K$; (ii) if $\varphi \lor \psi \in K$, then $\varphi, \psi \in K$; (iii) if $\exists x. \varphi(x) \in K$, then for every term $t$, $\varphi(t) \in K$. Let $K$ be a complexity class of cut-formulas. We write $\delta \vdash_{K} A$ for a proof $\delta$ of $A$ such that the cut-formulas appearing in the proof $\delta$ are all in $K$.

2. Reduction of cut-formulas

Let $C_0$ be a given complexity class. A $C_0$-formula is a formula of $C_0$. Let $C'_0$ be the smallest extension of $C_0$ such that $C'_0$ is closed under positive connectives, i.e. (i) $C_0 \subseteq C'_0$; (ii) if $\varphi, \psi \in C'_0$, then $\varphi \land \psi \in C'_0$; (iii) if $\varphi(t) \in C'_0$, then $\exists x. \varphi(x) \in C'_0$. Let $C''_0$ denote the set of the formulas which are in $C'_0$ but not in $C_0$. Let $C_1$ be the smallest complexity class containing $C'_0$ (with the property that $\varphi \in C'_0$ implies $\{\varphi, \neg \varphi\} \subseteq C_1$).

**Definition 2.1.** Let $\Gamma$ be a set of formulas and $\delta$ be a proof. The number of occurrences of non-positive $C_0$-subformulas of $\Gamma$ that also are source formulas of $\Gamma$ in $\delta$, denoted by $n(C_0, \delta, \Gamma)$, is defined as follows:

- The last rule of $\delta$ is the axiom:
  $n(C_0, \delta, \Gamma) = 0$.
- The last rule of $\delta$ is a positive rule with the principal formula in $\Gamma$:
  Let $\delta'$ be the immediate subproof of $\delta$ with $\varphi$ as the source formula of the principal formula.
  $n(C_0, \delta, \Gamma) = n(C_0, \delta', \Gamma) + 1$ else $n(C_0, \delta, \Gamma \cup \{\varphi\})$.
- The last rule of $\delta$ is not a positive rule with the principal formula in $\Gamma$:
  Let $\delta_1, \ldots, \delta_k$ be the immediate subproofs of $\delta$.
  $n(C_0, \delta, \Gamma) = n(C_0, \delta_1, \Gamma) + \cdots + n(C_0, \delta_k, \Gamma)$.

The set $\Gamma$ in $n(C_0, \delta, \Gamma)$ is meant to be a subset of $C''_0$ and $\varphi \in C''_0$ entails that $\varphi$ is a positive formula. Given a proof $\delta \vdash_{C_1} A$, $\Gamma$ with $\Gamma \subseteq C'_0$, $n(C_0, \delta, \Gamma)$ corresponds to the number of occurrences of the maximal non-positive subformulas that contribute to the formation of $\Gamma$. It could also be related to the number of contractions that contribute
to the formation of $\Gamma$, however in our proof system, contraction of formulas is implicit, since we are considering sets of formulas.

**Lemma 2.1.** If $\delta \vdash_{[C_1]} \Delta, \Gamma$ with $n(C_0, \delta, \Gamma) = 0$ and $\Gamma \subseteq C_0''$, there is a proof $\delta' \vdash_{[C_1]} \Delta$ such that $\|\delta'\| \leq \|\delta\|$ and $|\delta'| \leq |\delta|$.

Proof by induction on $|\delta|$. Obviously the lemma holds when $|\delta| = 1$. Assume as the induction hypothesis that the lemma holds when $|\delta| = n + 1$. There are the following cases:

- The last rule of $\delta$ is a positive rule with the principal formula in $\Gamma$:
  
  Let $\delta_0 \vdash_{[C_1]} \Delta, \Gamma, \phi$ be the immediate subproof of $\delta$.

  Since $n(C_0, \delta, \Gamma) = 0$, we have $\phi \in C_0''$ and $n(C_0, \delta_0, \Gamma \cup \{\phi\}) = 0$. We apply the induction hypothesis on $\delta_0$ to derive a proof $\delta''$ of $\Delta$ with length $\|\delta''\| \leq \|\delta_0\| \leq \|\delta\|$ and depth $|\delta''| \leq |\delta_0| \leq |\delta|$.

- The last rule of $\delta$ is not a positive rule with the principal formula in $\Gamma$:

  Let $\delta_1 \vdash_{[C_1]} \Delta_1, \Gamma_1 \ldots, \delta_k \vdash_{[C_1]} \Delta_k, \Gamma_k$ be the immediate subproofs of $\delta$.

  Since $n(C_0, \delta, \Gamma) = 0$, we have $n(C_0, \delta_i, \Gamma_i) = 0$ for $i = 1, \ldots, k$. We apply the induction hypothesis on $\delta_i$ to derive a proof $\delta'_i$ of $\Delta_i$ with length $\|\delta'_i\| \leq \|\delta_i\|$ and depth $|\delta'_i| \leq |\delta_i|$. By combining these proofs, we obtain a proof of $\Delta$ with length $\|\delta\|$ and depth $|\delta|$.

Let $c(\Gamma)$ denote the closure of $\Gamma$ with respect to the positive connectives, i.e. (i) $\Gamma \subseteq c(\Gamma)$; (ii) if $\phi \vee \psi \in c(\Gamma)$, then $\phi, \psi \in c(\Gamma)$; (iii) if $\exists x \phi(x) \in c(\Gamma)$, then for every term $t$, $\phi(t) \in c(\Gamma)$. If $\Gamma \subseteq C_0''$, then a formula in $c(\Gamma) \cap C_0$ is a maximal non-positive subformula of some formula of $\Gamma$.

**Lemma 2.2.** If $\delta \vdash_{[C_1]} \Delta, \Gamma$ with $n(C_0, \delta, \Gamma) = k + 1$ and $\Gamma \subseteq C_0''$, there is a proof $\delta' \vdash_{[C_1]} \Delta, \Gamma, \phi' \vdash_{[C_1]} \Delta, \Gamma$ such that $n(C_0, \delta', \Gamma) \leq k, \|\delta'\| \leq \|\delta\| - 1$ and $|\delta'| \leq |\delta|$.

Proof by induction on $|\delta|$. Obviously the lemma holds when $|\delta| = 1$, since in this case $n(C_0, \delta, \Gamma) = k + 1$ does not hold. Assume as the induction hypothesis that the lemma holds when $|\delta| = n$. We prove that the lemma holds when $|\delta| = n + 1$. There are the following cases:

- The last rule of $\delta$ is a positive rule with the principal formula in $\Gamma$:

  Let $\delta_0 \vdash_{[C_1]} \Delta, \Gamma, \phi$ be the immediate subproof of $\delta$.

  Since $n(C_0, \delta, \Gamma) = k + 1$, we have either $\phi \in C_0''$ and $n(C_0, \delta_0, \Gamma \cup \{\phi\}) = k + 1$ or $\phi \notin C_0$ and $n(C_0, \delta_0, \Gamma \cup \{\phi\}) = k$. In the latter case, the lemma holds by setting $\phi' = \phi$ and $\delta' = \delta_0$. In the former case, we apply the induction hypothesis on $\delta_0$ to derive a proof $\delta'' \vdash_{[C_1]} \Delta, \Gamma, \phi \vdash_{[C_1]} \Delta, \Gamma$ with $n(C_0, \delta_0', \Gamma \cup \{\phi\}) \leq k, \|\delta''\| \leq \|\delta_0\| - 1$ and $|\delta''| \leq |\delta_0|$. The proof $\delta'' \vdash_{[C_1]} \Delta, \Gamma, \phi'$ is then constructed from $\delta_0'$ with $n(C_0, \delta', \Gamma) \leq k, \|\delta'\| \leq \|\delta\| - 1$ and $|\delta'| \leq |\delta|$.

- The last rule of $\delta$ is not a positive rule with the principal formula in $\Gamma$:

  Let $\delta_1 \vdash_{[C_1]} \Delta_1, \Gamma_1 \ldots, \delta_m \vdash_{[C_1]} \Delta_m, \Gamma_m$ be the immediate subproofs of $\delta$.

  We have $n(C_0, \delta_1, \Gamma_1) + \ldots + n(C_0, \delta_m, \Gamma_m) = k + 1$. Assume $n(C_0, \delta_i, \Gamma_i) = \delta_k + 1 > 0$. We apply the induction hypothesis on $\delta_i$ to derive a proof $\delta''_i \vdash_{[C_1]} \Delta_i, \Gamma_i, \phi' \vdash_{[C_1]} \Delta_i, \Gamma_i$ with $n(C_0, \delta_i', \Gamma_i) \leq k, \|\delta''_i\| \leq \|\delta_i\| - 1$ and $|\delta''_i| \leq |\delta_i|$. The proof $\delta'' \vdash_{[C_1]} \Delta, \Gamma, \phi'$ is then constructed from $\delta_1, \ldots, \delta_i - 1, \delta_i', \delta_i + 1, \ldots, \delta_m$ with $n(C_0, \delta', \Gamma) \leq k, \|\delta''\| \leq \|\delta\| - 1$ and $|\delta''| \leq |\delta|$.

**Lemma 2.3.** If $\delta \vdash_{[C_1]} \Delta, \neg \phi \in C_0''$, then for every $\phi' \in c(\{\phi\}) \cap C_0$, there is a proof $\delta' \vdash_{[C_1]} \Delta, \neg \phi' \vdash_{[C_1]} \Delta, \neg \phi'$ such that $\|\delta'\| \leq \|\delta\|$ and $|\delta'| \leq |\delta|$.

This lemma is basically the same as the second inversion lemma in [21] and the proof is omitted.

**Definition 2.2.** The relation $<$ on pairs of numbers is defined as follows: $(a_0, a_1) < (b_0, b_1)$ iff $a_0 < b_0$ or $a_0 = b_0$ and $a_1 < b_1$.

For the relation $\leq$, we have $(a_0, a_1) \leq (b_0, b_1)$ iff $(a_0, a_1) < (b_0, b_1)$ or $(a_0, a_1) = (b_0, b_1)$.

**Definition 2.3.** The function $n_0(C_0, \delta)$ mapping the set of the proofs with cut-formula complexity class $C_0$ to natural numbers is defined as follows:

- $n_0(C_0, \delta) = n(C_0, \delta_0, \{\phi\})$, if the last rule of $\delta$ is the cut rule with $\phi \in C_0''$ as the positive cut-formula of the rule and $\delta_0$ as the subproof of $\phi$ leading to $\phi$.

- $n_0(C_0, \delta) = 0$, if the last rule of $\delta$ is not the cut rule or is the cut rule without any of its cut-formulas in $C_0''$. 
**Theorem 2.1.** If $\delta \vdash_{C_1} A$, then there is a proof $\delta' \vdash_{C_0} A$ with $\|\delta'\| \leq \|\delta\|^{|\delta|}$ and $|\delta'| \leq |\delta|$.  

Proof by induction on $(|\delta|, n_0(C_0, \delta))$. Obviously the theorem holds when $|\delta| = 1$. In another words, it holds when $(|\delta|, n_0(C_0, \delta)) \leq (1, k)$ for all $k \geq 0$. Assume as the induction hypothesis that the theorem holds when $(|\delta|, n_0(C_0, \delta)) \leq (n, k)$ for all $k \geq 0$. We prove that the theorem holds when $(|\delta|, n_0(C_0, \delta)) = (n + 1, k)$ for all $k \geq 0$ by induction on $k$. If the last rule of $\delta$ is not the cut-rule or is the cut-rule with the cut-formulas in $C_0$, we apply the induction hypothesis directly. Otherwise, let $\delta_0 \vdash_{C_1} A$, $\varphi$ and $\delta_1 \vdash_{C_1} A$, $\neg \varphi$ be the two immediate subproofs of $\delta$. Without loss of generality, we may assume $\varphi \in C_0$. For $k = 0$, we construct $\delta'$ as follows:

- **Lemma 2.2** is applied to the construction of $\delta'_0 \vdash_{C_1} A$ with $\|\delta'_0\| \leq \|\delta_0\|$ and $|\delta'_0| \leq |\delta_0|$. 
- The induction hypothesis is then applied to the construction of $\delta' \vdash_{C_0} A$ with $\|\delta'\| \leq \|\delta_0\|^{|\delta'_0|} \leq \|\delta\|^{|\delta|}$ and $|\delta'| \leq |\delta_0|$.  

Assume as the new induction hypothesis that the theorem holds when $(|\delta|, n_0(C_0, \delta)) \leq (n + 1, k)$. We then prove that the theorem holds when $(|\delta|, n_0(C_0, \delta)) = (n + 1, k + 1)$ as follows.

- **Lemma 2.2** is applied to the construction of $\delta'_0 \vdash_{C_1} A$, $\varphi$, $\varphi'$ for some $\varphi' \in c((\varphi)) \cap C_0$ such that $n(C_0\delta'_0, \{\varphi\}) \leq k$, $\|\delta'_0\| \leq \|\delta_0\| - 1$ and $|\delta'_0| \leq |\delta_0|$. By combining $\delta'_0$ and $\delta_1$, and then according to the induction hypothesis, we have a proof $\delta''_0 \vdash_{C_0} A$, $\varphi'$ with $\|\delta''_0\| \leq (\|\delta'_0\| + \|\delta_1\| + 1) = (\|\delta_0\| + \|\delta_1\|) = \|\delta\|$ and $\|\delta''_0\| \leq \|\delta_0\| + \|\delta_1\| + 1 \leq \|\delta_0\| + \|\delta_1\|$.  

- **Lemma 2.3** is applied to the construction of $\delta''_0 \vdash_{C_1} A$, $\neg \varphi'$ such that $\|\delta''_0\| \leq \|\delta_0\|$ and $|\delta''_0| \leq |\delta_0|$. By the induction hypothesis, we have a proof $\delta''_0 \vdash_{C_0} A$, $\neg \varphi'$ with $\|\delta''_0\| \leq \|\delta_0\|^{|\delta''_0|} \leq |\delta_0| |\delta''_0| \leq |\delta_1|$ and $\|\delta''_0\| \leq \|\delta_0\| + \|\delta_1\| + 1 \leq \|\delta_0\| + \|\delta_1\|$. By combining $\delta''_0$ and $\delta''_1$, we have a proof $\delta' \vdash_{C_0} A$ with $\|\delta'\| = \|\delta''_0\| + \|\delta''_1\| + 1 \leq \|\delta\| (\text{since } |\delta| \geq 2)$ and $|\delta'| \leq \max(|\delta''_0|, |\delta''_1|) + 1 \leq |\delta|$. This concludes the proof.

Let $O(f(n))$ (respectively, $\Omega(f(n))$) denote a function that grows at most (at least) as fast as $c \cdot f(n)$ for some real $c > 0$ (a context dependent number). We use $\Theta(f(n))$ to denote a function $g(n)$ such that $g(n) = O(f(n))$ and $g(n) = \Omega(f(n))$ at the same time. In the following, we discuss asymptotic properties of the proof length and the proof depth in cut-elimination. A proof is understood as a proof in a family of proofs with the length as the asymptotic factor in the family.

**Definition 2.4.** A proof $\delta$ is balanced, if $|\delta| = \Theta(2^{c-|\delta|})$ for some $c > 0$.

If we start with a balanced proof for the reduction of the complexity of cut-formulas, the following upper bound of the proof length can be inferred from the theorem.

**Corollary 2.1.** If $\delta \vdash_{C_1} A$ is a balanced proof, then there is a proof $\delta' \vdash_{C_0} A$ with $\|\delta'\| = \|\delta\|^{|\delta|/\ln(|\delta|)}$ and $|\delta'| = 2^{\Omega(|\delta|)}$.

**Definition 2.5.** A proof $\delta$ is unbalanced, if $|\delta| = \Theta(|\delta|^c)$ for some $c \geq 1$. $c$ is called the unbalance-degree of $\delta$.

If we start with an unbalanced proof for the reduction of the complexity of cut-formulas, the following upper bound of the proof length can be inferred from the theorem.

**Corollary 2.2.** If $\delta \vdash_{C_1} A$ is an unbalanced proof with unbalance-degree $c$, then there is a proof $\delta' \vdash_{C_0} A$ with $\|\delta'\| = 2^{\frac{c}{2} \cdot \|\delta\|^{|\delta|}}$ and $|\delta'| = O(|\delta|^c)$.

Although the growth rates of $\|\delta'\|^{|\delta|/\ln(|\delta|)}$ and $\|\delta\|$ are generally not comparable with $c \geq 1$, we have $\|\delta'\| = 2^{O(|\delta|)}$, since $\|\delta\|^{3/2} \cdot \ln(|\delta|) = O(|\delta|)$ when $c > 1$ and $\|\delta'\| \leq 2^{\|\delta\|^c} = 2^{O(|\delta|^c)}$ when $c = 1$.

3. Discussion

We first define a function for checking whether a formula is positive and a function for counting the number of alternations of formulas.
**Definition 3.1.** The function \( p(\varphi) \) mapping the set of formulas to \([0, 1]\) is defined as follows: \( p(\varphi) = 1 \) iff \( \varphi \) is a positive formula.

**Definition 3.2.** The function \( z(\varphi) \) is the number of alternations of \( \varphi \) defined as follows:

- \( z(\varphi) = 1 \), if \( \varphi \) is a literal.
- \( z(\varphi \lor \psi) = \max(z(\varphi) + 1 - p(\varphi), z(\psi) + 1 - p(\psi)) \).
- \( z(\varphi \land \psi) = z(\neg \varphi \lor \neg \psi) \).
- \( z(\exists x. \varphi(x)) = z(\varphi(x)) + 1 - p(\varphi(x)) \).
- \( z(\forall x. \varphi(x)) = z(\exists x. \neg \varphi(x)) \).

A pure formula is a formula such that the binary connectives and quantifiers in the formula are all of the same type. A formula \( \varphi \) is a pure formula if and only if \( z(\varphi) = 1 \) (including the special case where \( \varphi \) is a literal and \( z(\varphi) = 1 \)).

**Theorem 3.1.** If \( \delta \vdash_{[\mathcal{P}_k]} \Delta \), then there is a proof \( \delta' \vdash_{[\mathcal{P}]} \Delta \) with \( |\delta'| \leq \|\delta\| \).

Although this upper bound of the depth is similar to that in Theorem 2.1, the strategy used for proving the theorem does not work in this case. We obtain Theorem 3.1 by using the same strategy as that used to prove that the depth is \( \leq 2^{|\delta|} \) in [21]. The proof of the theorem is similar to that of the corresponding theorem in [21] and is therefore omitted.

Let \( \mathcal{P}_k \) denote the complexity class such that \( \varphi \in \mathcal{P}_k \) iff \( z(\varphi) \leq k \).

**Definition 3.3.** The function \( \text{pd}(n, a, b) \) mapping triples of numbers to numbers indicating the upper bound of the proof depth of cut-free proofs constructed from proofs with depth \( a \), length \( b \), and cut-formulas in \( \mathcal{P}_n \), is defined as follows:

- \( \text{pd}(0, a, b) = a \)
- \( \text{pd}(1, a, b) = b \)
- \( \text{pd}(2, a, b) = \text{pd}(n + 3, a, b) = \text{pd}(n + 2, b, b^a) \) for \( n \geq 0 \).

By combining Theorems 2.1 and 3.1, we obtain the following corollary.

**Corollary 3.1.** If \( \delta \vdash_{[\mathcal{P}_k]} \Delta \), then there is a proof \( \delta' \vdash_{[\mathcal{P}]} \Delta \) with \( |\delta'| \leq \text{pd}(k, |\delta|, \|\delta\|) \).

Suppose that we start with a proof-tree with depth \( n \) (which implies that the length is at most \( 2^n \)) and cut-formulas of complexity \( k \) (using the number of alternations as the measure of the complexity). Some examples of the upper bounds of the proof depth of cut-elimination are as follows:

<table>
<thead>
<tr>
<th>( k )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
<th>( 5 )</th>
<th>( 6 )</th>
<th>( 7 )</th>
<th>( 8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depth</td>
<td>( 2^O(n) )</td>
<td>( 2^O(n) )</td>
<td>( 2^O(n)^2 )</td>
<td>( 2^{2^O(n)} )</td>
<td>( 2^{2^O(n)^2} )</td>
<td>( 2^{2^{2^O(n)}} )</td>
<td>( 2^{2^{2^O(n)^2}} )</td>
<td></td>
</tr>
</tbody>
</table>

If we restrict the initial proof-tree to be totally unbalanced (unbalance-degree 1) with depth \( n \) (length \( O(n) \)), we obtain the following table of the upper bounds of the proof depth:

<table>
<thead>
<tr>
<th>( k )</th>
<th>( 1 )</th>
<th>( 2 )</th>
<th>( 3 )</th>
<th>( 4 )</th>
<th>( 5 )</th>
<th>( 6 )</th>
<th>( 7 )</th>
<th>( 8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Depth</td>
<td>( O(n) )</td>
<td>( O(n) )</td>
<td>( 2^{O(n)} )</td>
<td>( 2^{O(n)} )</td>
<td>( 2^{O(n)^2} )</td>
<td>( 2^{2^{O(n)}} )</td>
<td>( 2^{2^{2^{O(n)}}} )</td>
<td>( 2^{2^{2^{O(n)^2}}} )</td>
</tr>
</tbody>
</table>
These tables show that the upper bound of the number of exponential increase of proof depth is basically half of the complexity of cut-formulas. This improves our knowledge on the number of exponential increase in the upper bound which was roughly the same as the complexity of cut-formulas.

4. Concluding remarks

This paper provides a refined view on cut-elimination and brings new insight into the relation between cut-formulas and short proofs. If we use the number of alternations as the measure of the complexity of cut-formulas, the upper bound of the number of exponential increase of proof depth is basically half of the complexity of cut-formulas. This paper also indicates the possible importance of binary connectives in cut-formulas when a mixture of quantifiers and binary connectives is used. Reducing one binary connective in each of the cut-formulas in a proof does not lead to exponential increase of proof length when the original proof is balanced, however it may lead to exponential increase when the original proof is unbalanced. Suppose that we have cut-formulas where quantifiers and binary connectives in a path of the cut-formulas (presented as binary trees) are in such a way that each quantifier is followed by a binary connective and each binary connective is followed by a quantifier (unless it is at the end of the path). Suppose further that two consecutive items are of different types. An illustration of a possible scenery of cut-elimination is as follows: (i) If we start with an unbalanced proof, eliminating one level of quantifiers (one in each cut-formula in one round), we may get a balanced proof with at most polynomial increase of the depth. Eliminating one level of binary connectives (one in each cut-formula) in the balanced proof does not cause any significant increase of the length nor of the depth (at most polynomial increase). (ii) Thereafter, when we start with the balanced proof (resulting from the previous step), eliminating one level of quantifiers, we may get an unbalanced proof with moderate increase of the length (at most quasi-polynomial). Eliminating one level of binary connectives in the unbalanced proof, we may get a balanced proof with approximately the same depth (at most linear increase) and an exponential increase in proof length. The first step transforms an unbalanced proof into a balanced proof and the second step is then repeated in order to produce a sequence of exponential increase of the proof depth (and also proof length). For some proofs, this kind of interplay between quantifiers and binary connectives as illustrated in the second step makes cut-formulas powerful with respect to obtaining short proofs with cuts.

Acknowledgements

The author thanks anonymous referees for their constructive suggestions, comments and error corrections that helped improving this paper.

References