# BRICS

Basic Research in Computer Science

BRICS RS-03-46 P. Gerhardy: The Role of Quantifier Alternations in Cut Elimination

# The Role of Quantifier Alternations in Cut Elimination

**Philipp Gerhardy**

**BRICS Report Series** **RS-03-46**

**ISSN 0909-0878** **December 2003**

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

# The Role of Quantifier Alternations in Cut Elimination

Philipp Gerhardy

December, 2003

**Abstract**

Extending previous results from the author's master's thesis, subsequently published in the proceedings of CSL 2003, on the complexity of cut elimination for the sequent calculus **LK**, we discuss the role of quantifier alternations and develope a measure to describe the complexity of cut elimination in terms of quantifier alternations in cut formulas and contractions on such formulas.

## 1 Introduction

In this note we will present an extension of results on the complexity of cut elimination in the sequent calculus **LK**, first developed in [1] and subsequently published in [2]. There it is shown how the complexity of cut elimination primarily depends on the nesting of quantifiers in cut formulas and contractions on ancestors of such cut formulas. A more complicated proof of the role of quantifier nestings was first given by Zhang in [4].

In this note we extend the analysis and develope a measure that describes with sufficient accuracy the role of quantifier alternations in cut elimination. The measure will be slightly more complicated than the notion of nested quantifier depth, $nqf$, described in [2], but will generalize with similar ease to incorporate the role of contractions. An earlier, more complicated treatment of the role of quantifier alternations by Zhang can be found in [5]. Though leading to comparable results, in particular the measure of the cut complexity described in [5] is far more complicated than the one presented in this note. For another attempt at defining a measure capturing quantifier alternations, albeit without accompanying proof of cut elimination, see Visser[3]. Neither Zhang nor Visser treat the role of contractions in the complexity of cut elimination.

# 2 Previous results

Let **LK** be the sequent calculus as defined in [2], i.e. with multiplicative rules and with no implicit contractions. Let $|\cdot|$ denote the depth and $||\cdot||$ the size of formulas and proofs, in the latter case not counting weakenings and contractions. Let $nqf(\cdot), dqf(\cdot)$ and $cnqf(\cdot)$ denote the nested quantifier depth, the deepest quantified formula (informally, the largest number of propositional connectives one has to "peel off" to get to a quantifier) and the contracted nested quantifier depth respectively, as defined in [2].

In [2] the following results are proved:

**Refined Reduction Lemma.** *Let $\phi$ be an* **LK***-proof of a sequent $\Gamma \vdash \Delta$ with the final inference a cut with cut formula $A$. Then if for all other cut formulas $B$*

*(i) $nqf(A) \geq nqf(B)$ and $dqf(\phi) = dqf(A) > dqf(B)$, then there exists a proof $\phi'$ of the same sequent with $dqf(\phi') \leq dqf(\phi) - 1$ and $|\phi'| \leq |\phi| + 1$.*

*(ii) $nqf(\phi) = nqf(A) > nqf(B)$ and $dqf(A) = 0$, then there exists a proof $\phi'$ of the same sequent with $nqf(\phi') \leq nqf(\phi) - 1$ and $|\phi'| < 2 \cdot |\phi|$.*

*If the cut formula $A$ is atomic and both subproofs are cut free, then there is a cut free proof $\phi'$ with $|\phi'| < 2 \cdot |\phi|$.*

**Lemma 1.** *Let $\phi$ be an **LK**-proof of a sequent $\Gamma \vdash \Delta$. If $dqf(\phi) = d > 0$, then there is a proof $\phi'$ of the same sequent with $dqf(\phi') = 0$ and $|\phi'| \leq 2^d \cdot |\phi|$.*

**Lemma 2.** *Let $\phi$ be an **LK**-proof of a sequent $\Gamma \vdash \Delta$. If $dqf(\phi) = 0$*

*and* $nqf(\phi) = d > 0$*, then there is a proof* $\phi'$ *of the same sequent with* $nqf(\phi') \leq d - 1$ *and* $|\phi'| < 2^{|\phi|}$.

**First Refined Cut Elimination Theorem.** *Let* $\phi$ *be an* **LK***-proof of a sequent* $\Gamma \vdash \Delta$*. If* $nqf(\phi) = d > 0$*, then there is a proof* $\phi'$ *of the same sequent and a constant* $c$*, depending only on the propositional nesting of the cut formulas, so that* $nqf(\phi') \leq d - 1$ *and* $|\phi'| \leq 2^{c \cdot |\phi|}$.

**Corollary 3.** *Let* $\phi$ *be an* **LK***-proof of a sequent* $\Gamma \vdash \Delta$ *and let* $nqf(\phi) = d$*. Then there is a constant* $c$*, depending only on the propositional nesting of the cut formulas, and a proof* $\phi'$ *of the same sequent where* $\phi'$ *is cut free and* $|\phi'| \leq 2_{d+1}^{c \cdot |\phi|}$.

**Contraction Lemma.** *Let* $\phi$ *be an* **LK***-proof of a sequent* $\Gamma \vdash \Delta$*, with* $nqf(\phi) > cnqf(\phi)$ *then there is proof* $\phi'$ *of the same sequent with* $nqf(\phi')$ $= cnqf(\phi')$ *and* $||\phi'|| \leq ||\phi||$*. As a consequence also* $|\phi'| \leq 2^{|\phi|}$

**Second Refined Cut Elimination Theorem.** *Let* $\phi$ *be an* **LK***-proof of a sequent* $\Gamma \vdash \Delta$*. Then there is a constant* $c$ *depending only on the propositional nesting of the cut formulas and a cut free proof* $\phi'$ *of the same sequent where* $|\phi'| \leq 2_{cnqf(\phi)+2}^{c \cdot |\phi|}$.

The main work is to prove the Refined Reduction Lemma and the Contraction Lemma from which the remaining results follow easily.

To sum up, first it is shown that the complexity of cut elimination primarily depends on the nesting of quantifiers in cut formulas, while the elimination of the propositional connectives has a negligible contribution to the complexity of cut elimination. As mentioned above this result was also shown by Zhang in [4]. Moreover, if for a cut formula none of the direct ancestors have been contracted, then the cut can be eliminated with low complexity by a mere rearrangement of the proof that does not increase the size of the proof. Thus the non-elementary complexity of cut elimination was shown to depend only on the nested quantifier depth of cut formulas whose ancestors, of sufficient quantifier depth, also have been contracted.

# 3 Quantifier alternations

In section 3.4 of [2] it is discussed that blocks of $\forall, \wedge$-connectives, respectively $\exists, \vee$, can be eliminated together, and it is shown that eliminating such a block from a cut formula at most doubles the depth of the proof. In [2] the following lemma is proved:

**Lemma 4.** *Let $\phi$ be a proof of a sequent $\Gamma \vdash \Delta$ with the last inference a cut. Let the cut formula be constructed from formulas $B_1, \ldots B_n$ by the connectives $\forall$ and $\wedge$ only (resp. $\exists$ and $\vee$). Then we can replace that cut by a number of smaller cuts with cut formulas $B_i$. For the resulting proof $\phi'$ we have $|\phi'| < 2 \cdot |\phi|$.*

This lemma immediately suggests a bound on cut elimination based on the number of alternations between such blocks. We propose the following cut elimination strategy : first we eliminate as many outermost propositional connectives as possible, next we eliminate all outermost $\forall, \wedge$ and $\exists, \vee$ blocks. Repeating this we eventually arrive at a cut free proof. By the Refined Reduction Lemma and subsequently Lemma 1, both of which can easily be adapted to some measure of number of quantifier alternations instead of $nqf$, we see that the first step, eliminating propositional connectives, is not critical for the complexity of cut elimination. However, defining a new appropriate complexity measure for this cut elimination strategy is not trivial, as can also be seen by the complicated measure defined by Zhang[5] in order to prove a comparable result.

We want to define a measure $aqf$, the alternating quantifier depth. First consider the following very naive approach: Let us restrict the logical connectives to $\forall, \exists, \wedge$ and $\vee$ and let us count the propositional connectives $\wedge, \vee$ as the quantifiers $\forall, \exists$. Defining the $aqf$ as the number of alternations between quantifier blocks in cut formulas would not give the desired result. Alternations between propositional connectives $\wedge, \vee$, which can be eliminated easily, would be perceived as alternations between quantifiers $\forall, \exists$, which are expensive to eliminate. Thus this definition of $aqf$ would lead to a bound on cut elimination much worse in such situations than the bound already achieved via the nested quantifier depth $nqf$.

In general it turns out to be difficult to define, inductively on the formula, a measure of cut complexity that correctly captures the role of quantifier alternations. The difficulty is to decide when to increase the alternating quantifier depth.

For example, when facing a formula composed of two subformulas and one of the propositional connectives, e.g. the connective $\vee$, it is non-trivial to decide or predict whether the connective is part of a block of propositional connectives, and hence relatively harmless with respect to the alternations already present in the two subformulas, or it marks the beginning of an $\exists, \vee$ block which should mark an increase in the number of alternations.

Consider the formula $A :\equiv B \vee C$, where the subformula $C$ is assumed to be purely $\forall, \wedge$:

- if $B$ is purely $\exists, \vee$ then
  - $aqf(A)$ should be 0 - eliminate the $\vee$ (simple), then two blocks each without alternations remain
  - $aqf(\exists x A)$ should be 1 - all the $\exists, \vee$ constitute one block, the $\forall, \wedge$ block below constitutes the alternation
  - $aqf(\forall x A)$ should be 1 - eliminate the $\forall$(expensive), eliminate the $\vee$(simple), eliminate the two alternation free blocks
- if $B$ has an outermost $\exists, \vee$ block and one $\forall, \wedge$ block below
  - $aqf(A)$ should be 1 - eliminate the $\vee$(simple) then one alternation remains
  - $aqf(\exists x A)$ should be 1 - all the $\exists, \vee$ constitute one block, the $\forall, \wedge$ blocks below constitute the alternation
  - $aqf(\forall x A)$ should be 2 - eliminate the $\forall$(expensive), eliminate the $\vee$(simple) and still one alternation remains in the subformula $B$

The example demonstrates the problem of deciding *inductively* on the formula when to increase the alternating quantifier depth. At the point of the propositional connective we might not yet have sufficient information to decide whether to increase or not. On the other hand postponing the decision until we meet the next quantifier requires information on the exact structure of the subformulas that may no longer be available.

The solution is to let the complexity measure mirror the intended cut elimination strategy. This leads to defining the measure $aqf$ for the cut complexity *recursively* on the cut formula instead of inductively:

- if $A$ is atomic, purely $\exists, \vee$ or purely $\forall, \wedge$ then $aqf(A) = 0$
- if $A$ is composed of formulas $B_1, \ldots, B_n$ (each with outermost connective a quantifier) by propositional connectives only then $aqf(A) = max\{aqf(B_i)\}$
- if $A(:= \forall x C$ for some $C)$ is composed of connectives $\forall, \wedge$ and formulas $B_1, \ldots, B_n$ (each with outermost connective $\exists, \vee$) then $aqf(A) = max\{aqf(B_i)\} + 1$
- if $A(:= \exists x C$ for some $C)$ is composed of connectives $\exists, \vee$ and formulas $B_1, \ldots, B_n$ (each with outermost connective $\forall, \wedge$) then $aqf(A) = max\{aqf(B_i)\} + 1$

Moreover we treat implication $B \rightarrow C$ as $\neg B \vee C$, and negation $\neg B$ simply flips the polarity of other connectives below, i.e. $\exists, \vee \mapsto \forall, \wedge$ and vice versa. With this definition of $aqf$ for formulas, we define $aqf$ for proofs:

**Definition 5.** $aqf(\phi) := \sup\{aqf(A) : A \text{ is a cut formula in } \phi\}$

Also the notion of deepest quantified formula $dqf$ defined in [2] can be adapted to $aqf$, yielding a version of the Refined Reduction Lemma with $aqf$ instead of $nqf$. Now it is easy to show the following theorem:

**Theorem 6.** *Let $\phi$ be an* **LK***-proof of a sequent $\Gamma \vdash \Delta$ and let $aqf(\phi) = d$. Then there is a constant $c$, depending only on the propositional blocks of the cut formulas, and a proof $\phi'$ of the same sequent where $\phi'$ is cut free and $|\phi'| \leq 2_{d+1}^{c \cdot |\phi|}$.*

**Proof:** The theorem follows from the cut elimination strategy described above, and adaptions of Lemma 1 and Lemma 2 to the measure $aqf$ instead of $nqf$. These adaptions follow from an adaption of the Refined Reduction Lemma to the measure $aqf$ as discussed above. □

The definition of $caqf$, the contracted alternating quantifier depth, is defined from $aqf$ in the same way $cnqf$ is defined from $nqf$ (see [2]). Thus also taking the role of contractions into account we get:

**Theorem 7.** *Let $\phi$ be an **LK**-proof of a sequent $\Gamma \vdash \Delta$. Then there is a constant $c$ depending only on the propositional blocks of the cut formulas and a cut free proof $\phi'$ of the same sequent where $|\phi'| \leq 2^{c \cdot |\phi|}_{caqf(\phi)+2}$.*

In conclusion both theorems follow easily from the analysis of cut elimination presented in [2], in particular Lemma 4, and the cut elimination strategy described above. As mentioned above a comparable result is proved in [5] but with a far more complicated complexity measure and a more complicated proof.

Furthermore, as with the upper bounds on cut elimination presented in [2], the bounds $aqf$ and $caqf$ are optimal with regards to Statman's lower bound example, i.e. the upper and the lower bound coincide. Conversely, one can say that every proof that yields an example of non-elementary cut elimination must use cut formulas with alternating quantifiers and contractions in a way similar to Statman's lower bound example.

Finally, the exponential bound on cut elimination in the case of pure $\forall, \wedge$-cuts, respectively $\exists, \vee$-cuts, that is stated in [2], follows as a special case from these bounds.

# 4 Comparison with the literature

In this section we will briefly discuss the measures for the number of quantifier alternations proposed by resp. Zhang[5] and Visser[3].

The measure defined by Zhang uses two formula classes $\delta$ and $\delta'$:

**Definition 8. (Zhang[5])** *A formula $B$ is in $\delta(A)$ iff*

- *$A = B$, or*
- *$A = C \wedge D$ and $B \in \delta(C) \cup \delta(D)$, or*

- *$A = \forall x C(x)$ and $B \in \delta(C(t))$ for any term $t$.*

**Definition 9. (Zhang[5])** *A formula $B$ is in $\delta'(A)$ iff*

- *$B \in \delta(A)$, and*
- *$B$ is either a disjunction of two formulas, or*
- *$B$ is an $\exists$-formula s.t. all terms occurring in $B$ also occur in $A$*

**Definition 10. (Zhang[5])** *The cut complexity $\rho(A)$ of a formula $A$ is defined as a polynomial in $w$ as follows:*

- *if $\delta'(A)$ is empty, then $\rho(A) := w$,*
- *if $\delta'(A) = \{B_i | 1 \leq i \leq n\}$ and there is a formula $C$ s.t. $\forall x C(x) \in \delta(A)$ and $nqf(C) \geq nqf(B_i)$ for $1 \leq i \leq n$, then $\rho(A) := (\rho(B_1) \oplus \ldots \oplus \rho(B_n)) \cdot w$,*
- *if $A = B \wedge C$, $\delta'(A) = \{B_i | 1 \leq i \leq n\}$ and there is no formula $C$ s.t. $\forall x C(x) \in \delta(A)$ and $nqf(C) \geq nqf(B_i)$ for $1 \leq i \leq n$, then $\rho(A) := (\rho(B) \oplus \rho(C)) + 1$,*
- *if $\delta'(A) = \{A\}$, then $\rho(A) := \rho(\neg A)$*

*where $\oplus$ is the operation of summing two polynomials by raising them to the same degree and then taking the pointwise maximum over their coefficients.*

The definition is somewhat similar to the definition of the alternating quantifier depth $aqf$ presented in this note, as the degree of the cut complexity polynomial corresponds to our notion of $aqf$.

In detail, the first item in the definition covers the case when the formula is atomic, purely $\forall, \wedge$ or (via the fourth item) purely $\exists, \vee$. The second item corresponds to eliminating a $\forall, \wedge$ block (or via the fourth item an $\exists, \vee$ block), and hence here the degree of the polynomial is increased. The third item corresponds to eliminating in-between propositional connectives, which only adds a constant to the polynomial.

The proof of cut elimination given the cut complexity polynomial above proceeds via several rather technical lemmas and uses an additional formula class $\delta^*$.

Visser defines a measure "depth of quantifierchanges" via a three place function $\varrho$ (p.281, [3]), where the first parameter is 0 when the formula under consideration occurs positively and 1 if it occurs negatively, the second parameter is 0 when we are in existential mode and 1 when we are in universal mode, while the last parameter is the formula under consideration.

The definition of $\varrho$ is as follows:

**Definition 11. (Visser[3])** *Let $\varrho(A)$ of a formula $A$ be $\varrho(0, 0, A)$ and let*

- $\varrho(i, j, A) := 0$ *of $A$ is atomic,*
- $\varrho(i, j, B \wedge C) = \varrho(i, j, B \vee C) := \max\{\varrho(i, j, B), \varrho(i, j, C)\}$
- $\varrho(i, j, \neg B) := \varrho(1 - i, 1 - j, B)$
- $\varrho(0, j, B \rightarrow C) := \max\{\varrho(1, 1 - j, B), \varrho(0, j, C)\}$
- $\varrho(1, j, B \rightarrow C) := \max\{\varrho(0, j, B), \varrho(1, 1 - j, C)\}$
- $\varrho(i, 0, \exists x B) := \varrho(i, 0, B)$
- $\varrho(i, 1, \exists x B) := \varrho(i, 0, B) + 1$
- $\varrho(i, 0, \forall x B) := \varrho(i, 1, B) + 1$
- $\varrho(i, 1, \forall x B) := \varrho(i, 1, B)$

The merit of the measure defined by Visser is that it treats negation and implication directly. Contrary to the measure defined by Zhang and the measure $aqf$ defined in this note, Visser's $\varrho$ makes no distinctions for the propositional connectives as to whether they appear in existential or universal mode, i.e. below an existential or a universal quantifier. Thus the measure $\varrho$ assigns the same "depth of quantifierchanges" to the formulas

$$\forall x(\forall y P(x, y) \vee \forall z Q(x, z))$$

and

$$\forall x(\forall y P(x,y) \wedge \forall z Q(x,z)).$$

However, one can show that the complexity of cut elimination for the two (cut) formulas is not the same, i.e. cut elimination for the second formula, which is purely $\forall, \wedge$, is simpler than cut elimination for the first formula $\forall x(\forall y P(x,y) \vee \forall z Q(x,z))$, which contains a disjunction.

Thus, although capturing the main ideas, namely that cut elimination mainly depends on quantifier alternations, the measure as it is defined in [3], is not optimal in all cases to estimate the complexity of cut elimination.

# 5 Acknowledgements

I am grateful to Lev Beklemishev, Ulrich Kohlenbach and Albert Visser for many useful discussions on the subject of this note.

# References

[1] Philipp Gerhardy, *Improved Complexity Analysis of Cut Elimination and Herbrand's Theorem*, Master's thesis, Aarhus, 2003.

[2] ———, *Refined Complexity Analysis of Cut Elimination*, Proceedings of the 17th International Workshop CSL 2003 (Matthias Baaz and Johann Makovsky, eds.), LNCS, vol. 2803, Springer-Verlag, Berlin, 2003, pp. 212–225.

[3] Albert Visser, *The unprovability of small inconsistency*, Arch. Math. Logic **32** (1993), 275–298.

[4] Wenhui Zhang, *Cut elimination and automatic proof procedures*, Theoretical Computer Science **91** (1991), 265–284.

[5] ———, *Depth of proofs, depth of cut-formulas and complexity of cut formulas*, Theoretical Computer Science **129** (1994), 193–206.

## Recent BRICS Report Series Publications

**RS-03-46** Philipp Gerhardy. *The Role of Quantifier Alternations in Cut Elimination*. December 2003. 10 pp. Extends paper appearing in Baaz and Makowsky, editors, *European Association for Computer Science Logic: 17th International Workshop*, CSL '03 Proceedings, LNCS 2803, 2003, pages 212-225.

**RS-03-45** Peter Bro Miltersen, Jaikumar Radhakrishnan, and Ingo Wegener. *On converting CNF to DNF*. December 2003. 11 pp. A preliminary version appeared in Rovan and Vojtás, editors, *Mathematical Foundations of Computer Science: 28th International Symposium*, MFCS '03 Proceedings, LNCS 2747, 2003, pages 612–621.

**RS-03-44** Anna Gál and Peter Bro Miltersen. *The Cell Probe Complexity of Succinct Data Structures*. December 2003. 17 pp. An early version of this paper appeared in Baeten, Lenstra, Parrow and Woeginger, editors, *30th International Colloquium on Automata, Languages, and Programming*, ICALP '03 Proceedings, LNCS 2719, 2003, pages 332–344.

**RS-03-43** Mikkel Nygaard and Glynn Winskel. *Domain Theory for Concurrency*. December 2003. 45 pp. To appear in a *Theoretical Computer Science* special issue on Domain Theory.

**RS-03-42** Mikkel Nygaard and Glynn Winskel. *Full Abstraction for HOPLA*. December 2003. 25 pp. Appears in Amadio and Lugiez, editors, *Concurrency Theory: 14th International Conference*, CONCUR '03 Proceedings, LNCS 2761, 2003, pages 383–398.

**RS-03-41** Malgorzata Biernacka, Dariusz Biernacki, and Olivier Danvy. *An Operational Foundation for Delimited Continuations*. December 2003. 21 pp.

**RS-03-40** Andrzej Filinski and Henning Korsholm Rohde. *A Denotational Account of Untyped Normalization by Evaluation*. December 2003. 29 pp.

**RS-03-39** Jörg Abendroth. *Applying $\pi$-Calculus to Practice: An Example of a Unified Security Mechanism*. November 2003. 35 pp.