

Julius-Maximilians-Universität Würzburg  
Institut für Informatik  
Lehrstuhl für Informatik IV  
Theoretische Informatik

**Bachelor Thesis**

**simulation of proof systems**

Nils Wisiol

submitted on May 11, 2012

supervisor:  
Dr. Christian Glaßer

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Preliminaries</b>	<b>4</b>
<b>3</b>	<b>A brief Overview of Proof Systems</b>	<b>5</b>
<b>4</b>	<b>A set in <math>\text{co-NEXP} \setminus \text{OPT}</math></b>	<b>6</b>
<b>5</b>	<b>Conclusion and future work</b>	<b>8</b>
	<b>Bibliography</b>	<b>10</b>

# 1 Introduction

Welcome to my bachelor's thesis. Based upon work of [Mes99].

## 2 Preliminaries

As mentioned before, we will first introduce important symbols and definitions. Although some familiarity with standard notions of complexity theory is assumed, here we will define most of the notions used in this thesis. For the most important ones, we will give a short discussion.

**Definition 1** (Proof system). *A function  $f \in \mathcal{FP}$  is called proof system for a language  $L$  if the range of  $f$  is  $L$ .*

**Definition 2** (OPT). *Let OPT be the complexity class of all sets that have a  $p$ -optimal proof system.*

### 3 A brief Overview of Proof Systems

After defining the important notions for this thesis, we will give a brief overview of the most important results in the field of optimal proof systems.

One basic lemma that is widely used establishes a connection between optimal proof systems and polynomial many-one-reducibility. Later in this thesis, we will use it to proof corollary 3. The following proof is mainly taken from Köbler et al. [KMT03].

**Lemma 1.** *If  $A$  has a  $(p)$ -optimal proof system and if  $B \leq_m^p A$ , then  $B$  has a  $(p)$ -optimal proof system, too.*

*Proof.* Let  $h$  be a  $p$ -optimal proof system for  $A$  and let  $B$  many-one reduce to  $A$  via  $f \in \mathcal{FP}$ , that is  $x \in B \Leftrightarrow f(x) \in A$ . Then  $h'$  defined by

$$h'(\langle x, w \rangle) = \begin{cases} x & (h(w) = f(x)), \\ \perp & (\text{otherwise}), \end{cases}$$

is a proof system for  $B$ , as  $h(w) = f(x) \in A$  is equivalent to  $x \in B$ . To show  $h'$  is optimal, let  $g'$  be a proof system for  $B$ . In order to obtain a proof system for  $A$ , let  $g$  be

$$g(bw) = \begin{cases} h(w) & (b = 0), \\ f(g'(w)) & (b = 1). \end{cases}$$

Since both  $h(w)$  and  $f(g'(w))$  are in  $A$  and  $h$  is a proof system for  $A$ ,  $g$  is also a proof system for  $A$ . As  $h$  is  $p$ -optimal, there is a function  $t \in \mathcal{FP}$  translating  $g$ -proofs to  $h$ -proofs implying that

$$h(t(1w)) = g(1w) = f(g'(w)).$$

This implies  $h'(\langle g'(w), t(1w) \rangle) = g'(w)$ . Hence,  $h'$   $p$ -simulates  $g'$ . □

## 4 A set in $\text{co-NEXP} \setminus \text{OPT}$

In this section, we will show that there are sets without optimal proof systems.

**Theorem 2.** *Let  $t : \mathbb{N} \rightarrow \mathbb{N}$  be a time-constructible function such that for every polynomial  $p$  there is a number  $n$  with  $p(n) \leq t(n)$ . Then there is a language  $L \in \text{co-NTIME}(t(n))$  that has no optimal proof system.*

Messner showed that under the same presumptions as in our theorem, there is a language  $L \in \text{co-NTIME}(t(n))$  without an optimal acceptor [Mes99]. He also proved that the existence of an optimal acceptor is equivalent to the existence of an optimal proof system for every p-cylinder  $L$ .

*Proof.* Let  $f_1, f_2, \dots$  be an enumeration of all  $\mathcal{FP}$ -functions with  $\text{time}(f_i) \leq n^i + i$ . For any  $i > 0$ , let  $L_i$  be the regular language described by the expression  $0^i 10^*$ . Define

$$L'_i = \{x \in L_i \mid \forall y \in \Sigma^* |y|^{2i} \leq t(|x|) \implies f_i(y) \neq x\}.$$

That is, as long as you put strings of length  $|y|^{2i} \leq t(|x|)$  into  $f_i$ , you will not obtain  $x$ . Let  $L = \bigcup_{i>0} L'_i$ .

How is that obtained?

First, we obtain  $L \in \text{co-NTIME}(t(n))$ . To show this, one considers

$$L \in \text{co-NTIME} \Leftrightarrow \overline{L} = \bigcup_{i>0} \overline{L'_i} = \bigcap_{i>0} \overline{L'_i} \in \text{NTIME}.$$

By negating the condition for  $L'_i$ , we get

$$\overline{L'_i} = \{x \in \Sigma^* \mid x \notin L_i \vee (\exists y \in \Sigma^* |y| \leq t(|x|) \wedge f_i(y) = x)\}.$$

For any given  $x$ , we can decide in polynomial time whether it is in any  $L_i$  or not. If it is not, then  $x$  is in  $\overline{L'_i}$  for all  $i > 0$  and therefore  $x \in \overline{L}$ , so we are done. If it is in any  $L_i$ , it is in exactly one  $L_i$ . Let  $i^*$  be the set with  $x \in L_{i^*}$ . We can simulate a deterministic polynomial-time machine calculating  $f_{i^*}(y)$  on every input  $y \in \Sigma^*$  with  $|y|^{2i^*} \leq t(|x|)$ . If, and only if, there is a path with  $f_{i^*}(y) = x$ , then  $x \in \overline{L}$ . In both cases,  $\overline{L} \in \text{NTIME}(t(n))$ .

For a proof system  $f_i$  with  $f_i(\Sigma^*) = L$ , we observe that  $L'_i = L_i$ . Assume there is an  $x = 0^i 1z \in L_i$  that is not in  $L'_i$ . Then there is an  $y$  with  $|y|^{2i} \leq t(|x|)$  and  $f_i(y) = x$ . Since  $f_i$  is a proof system for  $L$ , this yields  $x = 0^i 1z \in L$  and so  $x \in L'_i$ , which contradicts the assumption. Therefore, for any  $y$  with  $f_i(y) = x \in L_i$  we know that  $|y|^{2i} > t(|x|)$ . Speaking informally, every proof system  $f_i$  for  $L$  is “slow” on  $L'_i \subset L$ .

Assume now, for contradiction, that  $f_i$  is an optimal proof system for  $L$ . Let  $g$  be a function defined as

$$g(bx) = \begin{cases} f_i(x) & (b = 0), \\ x & (b = 1 \text{ and } x = 0^i 10^* \in L_i = L'_i). \end{cases}$$

$g$  is a proof system for  $L$  with polynomial length-bounded proofs for all  $x \in L_i$ . As  $f_i$  is optimal, there is a function  $f^*$  such that for all  $x \in L'_i$ ,  $f_i(f^*(x)) = g(x)$  and  $|f^*(x)| \leq p(|x|)$  for a polynomial  $p$ . Let  $q$  be the polynomial  $q(n) = p(n)^{2i}$ . As  $p(|x|)$  is positive,  $p(|x|) \leq p(|x|)^{2i}$ . As there is an  $n$  with  $q(n) \leq t(n)$ , there is an  $x$  in  $L_i$  such that  $|f^*(x)| \leq p(|x|) \leq q(|x|) = p(|x|)^{2i} \leq t(|x|)$ . According to the definition of  $L'_i$ , this yields  $f_i(f^*(x)) \neq x$ . Therefore,  $f_i$  is not optimal on  $L'_i$ , which contradicts the assumption that  $f_i$  is optimal on  $L$ .  $\square$

Now, let us take a closer look at this set  $L$  that has no optimal proof system. One first observation is that  $L$  is sparse. As every  $L'_i$  only contains strings that are of the form  $0^i10^*$ ,  $L$  is a subset of the regular language  $L_R = 0^*10^*$ . Therefore, the density of  $L_R$  is an upper bound for the density of  $L$ . As  $\text{dens}_{L_R}(n) = n$ ,  $L_R$  and  $L$  are both sparse.

[KMI98] showed that, for any nonempty sets  $L$  and  $A$  with  $L \leq_m^p A$ , if  $A$  has a optimal proof system, then  $L$  also has a optimal proof system. Together with this result, we obtain

**Corollary 3.** *No set  $\leq_m^p$ -hard for co-NE has an optimal proof system.*

Is this possible for  
co-NEXP?

*Proof.* With  $t(n) = 2^n$ , we can get an  $L \in \text{co-NE}$  that has no optimal proof system. Any  $\leq_m^p$ -hard set  $A$  for co-NE is  $L \leq_m^p A$ . Together with the cited result we obtain, that  $A$  cannot have optimal proof system.  $\square$

## 5 Conclusion and future work

What a great work!



Hiermit versichere ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen Hilfsmittel und Quellen als die angegebenen benutzt habe. Weiterhin versichere ich, die Arbeit weder bisher noch gleichzeitig einer anderen Prüfungsbehörde vorgelegt zu haben.

Würzburg, den \_\_\_\_\_, \_\_\_\_\_  
(Nils Wisiol)

# Bibliography

- [KMI98] Johannes Köbler, Jochen Messner, and Abteilung Theoretische Informatik, *Complete problems for promise classes by optimal proof systems for test sets*, In Proc. 13th Annual IEEE Conference on Computational Complexity, CC 98, IEEE, 1998, pp. 132–140.
- [KMT03] Johannes Köbler, Jochen Messner, and Jacobo Torán, *Optimal proof systems imply complete sets for promise classes*, Inf. Comput. **184** (2003), no. 1, 71–92.
- [Mes99] Jochen Messner, *On optimal algorithms and optimal proof systems*, Proceedings of the 16th annual conference on Theoretical aspects of computer science (Berlin, Heidelberg), STACS'99, Springer-Verlag, 1999, pp. 541–550.