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

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.

Let $\Sigma = \{0,1\}$ denote the alphabet. The output of a Turing transducer M on input $x \in \Sigma^*$ is denoted by $M(x)$. If the transducer M does not accept or runs forever on input x, we define $M(x) = \perp$. We say a Turing transducer *calculates* a partial function f, if $M(x) = f(x)$ for all $x \in \Sigma^*$. We further define $\mathrm{time}_M(x)$ as the number of steps the transducer M runs on input $x \in \Sigma^*$. Similar, for a partial function f, we define $\mathrm{time}_f(x) = \mathrm{time}_M(x)$ for a transducer M calculating f. With $\mathcal{FP}$, we denote the set of all partial functions f with $\mathrm{time}_f(x) \leq p(|x|)$ for a polynomial p.

is that well-defined?

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.*

With these notions, we will take a look at important results in the field of optimal proof systems in the next chapter. For notions not defined in this thesis, refer to a standard work of computational complexity like the one from Papadimitriou [Pap94].

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 co-NEXP $\setminus$ OPT

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

Theorem 2. *Let $t : \mathbb{N} \to \mathbb{N}$ be a time-constructible function such that for every polynomial p there is a number n with $p(n) \le t(n)$. Then there is a language $L \in$ 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 $L \in$ co-NTIME$(t(n))$ without an optimal acceptor [Mes99]. He also proofed that the existence of a optimal acceptor is equivalent to the existence of a optimal proof system for every p-cylinder L.

Proof. Let $f_1, f_2, ...$ be a enumeration of all $\mathcal{FP}$-functions with time$(f_i) \le n^i + i$. For any $i > 0$, let L_i be the regular language described by the expression 0^i10^*. Define

How is that obtained?

$$L_i' = \{x \in L_i | \forall_{y \in \Sigma^*} |y|^{2i} \le t(|x|) \implies f_i(y) \neq x\}.$$

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

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

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

By negating the condition for L_i', we get

$$\overline{L_i'} = \{x \in \Sigma^* | x \notin L_i \vee (\exists_{y \in \Sigma^*} |y| \le t(|x|) \wedge f_i(y) = x)\}.$$

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 $|y|^{2i} \le t(|x|)$. If, and only if, there is a path with $f_{i^*}(y) = x$, then $x \in \overline{L}$. In both cases, $\overline{L} \in$ 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 $x = 0^i1z \in L_i$ that is not in L_i'. Then there is an y with $|y|^{2i} \le t(|x|)$ and $f_i(y) = x$. Since f_i is a proof system for L, this yields $x = 0^i1z \in L$ 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 a optimal proof system for L. Let g be a function defined as

$$g(bx) = \begin{cases} f_i(x) & (b = 0), \\ x & (b = 1 \text{ and } x = 0^i10^* \in L_i = L_i'). \end{cases}$$

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 $|f^*(x)| \le p(|x|)$ for a polynomial p. Let q be the polynomial $q(n) = p(n)^{2i}$. As $p(|x|)$ is positive, $p(|x|) \le p(|x|)^{2i}$. As there is an n with $q(n) \le t(n)$, there is an x in L_i such that $|f^*(x)| \le p(|x|) \le q(|x|) = p(|x|)^{2i} \le t(|x|)$. 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. □

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 $\mathrm{dens}_{L_R}(n) = n$, 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 $L \in$ 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. □

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.

[Pap94] Christos H. Papadimitriou, *Computational complexity*, Addison-Wesley, 1994.