Aalto University

Prof. Dr. Christopher Brzuska
Dept. of Mathematics and Syst. Analysis
Department of Computer Science
Aalto University School of Science
P.O. Box 11100
FI-00076 Espoo, Finland
+358 50 445 0136
chris.brzuska@aalto.fi
www.chrisbrzuska.de

August 22, 2021

Report: Veronika Slìvovà, *On the Complexity of Search Problems with a Unique Solution*

Dear colleagues,

Veronika's thesis studies search problems with unique solutions. Search problems with unique solutions arise in cryptography and complexity theory and can often help us understand the hardness of a problem better. E.g., problems with unique solutions allow us to measure how close a solution attempt is to *the* solution (rather than just *a* solution). For NP-complete problems, Valiant and Vazirani show a randomized reduction which turns any instance of an NP-problem into a problem which (1) has a unique solution with high probability and (2) where this solution is also a solution to the original problem. In this way, solving NP problems with unique solutions implies being able to solve all NP-problems.

Veronika's thesis is motivated by deepening our understanding of *search* problems with unique solutions. E.g., an injective one-way function in cryptography defines such a problem. However, an injective one-way function does not require that image values are easy to recognize and thus (potentially) encodes a search and decision problem at the same time. Veronika is particularly interested in understanding the relation between this kind of "mixed" search/decision problems and problems which are "only" search problems, captured by the class of total functions from NP (TFNP). The thesis contributes to our understanding of search problems with unique solutions via several results, falling broadly into two categories, placing a *concrete problem* in smaller complexity classes than previously known and investigating *relations* between *classes* of problems.

Complexity of a concrete problem

ARRIVAL. Veronika shows that the ARRIVAL problem on directed graphs lies not only in $\mathbf{NP} \cap \mathbf{coNP}$, but actually in $\mathbf{UP} \cap \mathbf{coUP}$, the analogous class with unique certificates. Moreover, Veronika establishes that ARRIVAL lies in **CLS**, a subclass of **TFNP**, improving over the known inlcusion of ARRIVAL in **PLS**.

Relations between classes of problems

TFNP vs. NP. Veronika's thesis establishes that the gap between TFNP and NP is hard to overcome, certainly in a black-box way. In a way, this result provides a formal underpinning to the difference between decision problems and "true" search problems.

TFNP vs. UP. In fact, Veronika shows the black-box separation for UP which is a natural strengthening to consider.

Average-case. Intesterestingly, Veronika also shows that not even assuming average-case hardness of **NP** or **UP** can help for using black-box techniques to build worst-case TFNP problems.

TFNP vs. injective OWF. Last, but not least, Veronika considers *injective one-way functions* and asks whether we base hard worst-case problems in TFNP on these. Conceptually, a separation might still be possible here since, as hinted above, injective one-way functions do not require an easy-to-recognize domain. Yet, cryptographic hardness tends to be rather strong and has been used, e.g., to prove the existence of hard learning problems. Veronika shows a separation for a restricted class of reductions called *simple*. I.e., she shows that via a simple black-box reduction, worst-case TFNP problems cannot be based on injective one-way functions.

Questions. Below, I include questions which I'd like to reflect upon with Veronika during the defense.

ARRIVAL. I found the results on ARRIVAL very interesting and thought about them in the context of derandomization. Namely, using Valiant-Vazirani, we can transform each **NP** problem into a **UP** problem via a *randomized* reduction, and likewise for **coNP** and **coUP**. In turn, Veronika's result does not require any randomness. Are there general lessons for us to learn from placing ARRIVAL in $\mathbf{UP} \cap \mathbf{coUP}$, e.g., about other graph problems in $\mathbf{coNP} \cap \mathbf{coNP}$?

TFNP. I found the separations in this thesis extremely interesting. Firstly, I am wondering whether Veronika thinks, as I do, that the separations are possible due to the missing "decision component" in the TFNP definition, or whether she sees different or additional conceptual reasons? Relatedly, I am curious whether she thinks that one could still prove a separation result for an injective one-way function whose range is efficiently checkable? By my understanding, the injective functions considered in Veronika's thesis are also pseudorandom generators and thus, their range is not efficiently checkable.

Evaluation. Veronika's results on ARRIVAL yield an improved understanding of its complexity as well as novel techniques for showing the uniqueness of certificates. In particular, the polynomial testability of run-profiles might have applications to similar graph problems.

Veronika's broad and general separation results for TFNP yield novel understanding of the class TFNP. Namely, the lack of "decision flavour" in the definition of the complexity class indeed makes TFNP quite unrelated to many other problems in cryptography, average-case and worst-case complexity. These insights can have consequences both for definitions of complexity classes as well as on the complexity problems we might use to build secure cryptography.

The thesis demonstrates Veronika's strong ability for creative scientific work and I strongly recommend to award the doctoral degree to Veronika.

With kind regards,

Prof. Dr. Christopher Brzuska
Assistant Professor
Department of Mathematics and Systems Analysis
Department of Computer Science
Aalto University School of Science
Finland