Dr. Klaus Scheicher
Institute of Mathematics
Augasse 2-6, 1090 Vienna
Austria
klaus.scheicher@boku.ac.at
+43 1 / 47654-5091

July 3, 2015

Prof. Dr. Libor Šnobl
Department of Physics
Czech Technical University
Břehová 7, 115 19 Prague 1
Czech Republic

Report on the habilitation thesis

Combinatorics on Words and Applications

By L'ubomíra Dvořáková.

The underlying habilitation thesis consists of six papers. Apart from paper [6], which is still under review, all papers have been published in top quality journals.

Roughly speaking, these papers can be grouped in three contexts. The papers [1, 2] cover topics from combinatorics on words and complexity of languages. The papers [3, 4] deal with the proof of a conjecture of Brlek and Reutenauer while in the papers [5, 6] the theory of Sturmian words is applied for the generation of psudo random numbers.

Ad [1, 2]. Let $\mathbf{u} = u_0u_1u_2\cdots$ be an infinite word over a finite Alphabet $\mathcal{A}$. A finite word w is called a factor of $\mathbf{u}$ if $\mathbf{u} = pws$, such that p is a finite and s is an infinite word. The language $\mathcal{L}(\mathbf{u})$ is the set of all of its factors. The set of factors of length n is denoted by $\mathcal{L}_n(\mathbf{u})$. The factor complexity $\mathcal{C}$ of $\mathbf{u}$ is the map $\mathbb{N} \mapsto \mathbb{N}$ defined by

$$\mathcal{C}(n) := \#\mathcal{L}_n(\mathbf{u}).$$

Morse and Hedlund proved that the factor complexity of aperiodic binary words is $\mathcal{C}(n) \geq n+1$. Sturmian words are defined to be aperiodic infinite binary words with minimal factor complexity.
In [1], the situation is analysed for alphabets with more than two letters. It turns out that this situation is much more complicated than in the binary case and most of the results known for binary sequences become wrong. This is mainly done by constructing the corresponding counterexamples.

In [2] the palindromic complexity

$$\mathcal{P}(n) = \#\{w \in \mathcal{L}_n(\mathbf{u}) : w \text{ is a palindrome } \}$$

is studied. In particular, a new characterisation of uniformly recurrent infinite words with finite defect is provided. The defect of an finite word w is defined to be the difference between the upper bound $|w| + 1$ and the number of palindromes contained in w. The defect of an infinite word w is defined to be the supremum over the defect of all of its prefixes.

Ad [3, 4]. Let $\mathbf{u}$ be an infinite word such that its language is closed under reversal. In this case, Brlek and Reutenauer conjectured, that the defect of the language can be expressed by the formula

$$2D(\mathbf{u}) = \sum_{n=0}^{\infty} T_{\mathbf{u}}(n), \quad \text{where} \quad T_{\mathbf{u}} = \Delta\mathcal{C}(n) + 2 - \mathcal{P}(n) - \mathcal{P}(n+1).$$

Brlek and Reutenauer could prove their conjecture only for periodic words. In [3], the candidate together with her coauthors, proved the conjecture for uniformly recurrent infinite words. Using completely different arguments, they established a full proof in [4].

Ad [5, 6]. It is a well known problem to design computational efficient pseudo random numbers generators (PRNGs). Most popular are so called linear congruential generators (LCGs). However, the main disadvantage of LCGs is their lattice structure: since every new element is computed recursively from a linear relation of order d from the previous elements, it follows immediately that consecutive elements of the sequence are located of a finite set of hyperplanes in the $d + 1$-dimensional space. In [5], combinatorics of words is applied to do away with this drawback.
Given two PRNGs (X_n), (Y_n) and a binary sequence (u_n), the binary sequence can be used as a switch between (X_n) and (Y_n) in order to construct a combined sequence with better distribution properties. Of course, the properties of the combined sequence depends on (X_n), (Y_n) and (u_n). In [5], it is proved that binary sequences (u_n) admitting the so called WELLDOC property produce combined sequences without lattice structure. Furthermore, explicit construction for such sequences are given. In [6], computational results of statistical tests of the PRNGs from [5] are presented.

In summary, I can assert that the candidate is doing research of high scientific quality. She authored more than 20 papers and got more then 40 citations all of them in top quality journals. She is well embedded in the international scientific community. Solving a well known problem from pure mathematics, she demonstrates her ability to identify and prove order in highly complicated situations. Moreover, she connects her research with recent aspects of applied computer science.

The contents of the underlying thesis provide an important contribution to current research.

I positively recommend the thesis for acceptance. It's a pleasure for me to recommend the candidate for promotion to the rank of Docent.

Sincerely,

Klaus Scheicher

Bibliography

[1] L'. Balková, E. Pelantová, and Š. Starosta. Sturmian jungle (or garden?) on multiliteral alphabets. *RAIRO Theor. Inform. Appl.*, 44(4):443–470, 2010.

[2] L'. Balková, E. Pelantová, and Š. Starosta. Infinite words with finite defect. *Adv. in Appl. Math.*, 47(3):562–574, 2011.

[3] L'. Balková, E. Pelantová, and Š. Starosta. On Brlek-Reutenauer conjecture. *Theoret. Comput. Sci.*, 412(41):5649–5655, 2011.

[4] L'. Balková, E. Pelantová, and Š. Starosta. Proof of the Brlek-Reutenauer conjecture. *Theoret. Comput. Sci.*, 475:120–125, 2013.

[5] L'. Balková, M. Bucci, A. de Luca, and S. Puzynina. Infinite words with well distributed occurrences. In *Combinatorics on words*, volume 8079 of *Lecture Notes in Comput. Sci.*, pages 46–57. Springer, Heidelberg, 2013.

[6] L'. Balková, M. Bucci, A. de Luca, J. Hladký, and S. Puzynina. Pseudorandom number generators based on infinite words. *submitted*, 2014.