Review on the habilitation thesis of Tatiana Jajcayová

Tatiana Jajcayová presents in her thesis a sample of her research work, built over five papers on different subjects in the interface of Computer Science and Mathematics.

The first two papers are devoted to geometric inverse semigroup theory. In the last decades, geometric group theory has been recognized as the most interesting subarea of algebra. For instance, 5 among the 18 laureates with the Abel Prize are famous for work in this area. Its success is probably due to the fact that it combines a geometric and an algorithmic viewpoint. Most of geometry is very poor algorithmically, so combinatorial/geometric group theory seemed to make the best of two worlds. This attracted attention from theoretical computer science as well, but from this other viewpoint groups seem a very particular case. After all, most functions are not permutations, and the algebraic structures which occur most naturally in theoretical computer science are semigroups/monoids. It was a matter of time until the emergence of geometric semigroup theory.

It must be said that arbitrary semigroups (which may be built from arbitrary functions like groups may be built from arbitrary permutations) have not provided so far (in my view) a convincing geometric theory. But geometric semigroup theory has already produced its jewels, and they lie within the realm of inverse semigroups/monoids. Inverse semigroups lie at an intermediate level between semigroups and groups: they may be built from injective functions. Like in the group case, they possess good algorithmics, associated with automata-theoretic methods, and can be used to classify certain features of topological spaces. It is a beautiful theory, but hard and demanding. If we compare free groups with free inverse semigroups, it is basically like going from words to trees, which means an upgrade in complexity, quite familiar to most computer scientists. Which know that there are good reasons to study trees.

Tatiana Jajcayová is one of the researchers which has made outstanding contributions to geometric inverse semigroup theory. This is the subject of the first two articles in her thesis.

The first article (Chapter 2) is devoted to HNN extensions of inverse semigroups. The main objectives of Tatiana's work on these have been to characterize Schützenberger graphs (the strongly connected components of the Cayley graph, which actually determine the full Cayley graph) under certain conditions and provide positive decidability results.

It must be said that HNN extensions and free products with amalgamation are arguably the most important constructions in geometric group theory due to their deep geometric meaning. Their generalization to inverse semigroup theory does not carry the same weight, but their importance is still great because both constructions have been in the frontline of the main combat: establishing the boundaries of (un)decidability. In fact, many decidability results from group theory cannot be directly generalized to groups, and this earned geometric inverse semigroup a reputation for being a hard subject with a small pay-off. Now Tatiana's results from Chapter 2 represent one of the best decidability results obtained so far.

In the second paper (Chapter 3), the maximal subgroups of free products with amalgamation of two finite inverse semigroups are computed. This is a remarkable tour-de-force which requires going very deep into the structure of these inverse semigroups. I note that understanding the maximal subgroups is one of the most important questions regarding any inverse semigroup. Why is this class of inverse semigroups important? The fact is that most of the success cases where the Schützenberger graphs are effectively constructible are either groups or inverse semigroups with finite Schützenberger graphs, or having trees as Schützenberger graphs. On the other hand, many free products with amalgamation of two finite inverse semigroups produce infinite Schützenberger graphs which are not trees (and they are not groups). I don't remember any instance where such a tough problem (characterizing the maximal subgroups) had been solved in such unfavourable circumstances.

The three remaining papers (Chapters 4 to 6) explore different subjects, not at all related to geometric inverse semigroup theory. They illustrate the broad scope of Tatiana's research interests.

Chapter 4 is about two problems in Cryptography, known as oblivious transfer and private information retrieval. The schemes proposed in the paper, based on the so-called p-subgroup assumption (applied to finite abelian groups), present advantages when compared with previously known schemes and can be considered as progress.

On the other hand, Chapter 5 features a generalization of difference sets where multiplicities are prescribed by a certain sequence of integers, named the frequency sequence. Difference sets, a very simple number-theoretic notion, has actually very interesting connections to Combinatorics (design theory), and a lot of intriguing problems arise by considering frequency sequences. This paper provides very pleasant lecture and it should be noted that among the results one can find an answer to a slight variation of an open problem proposed by Erdös himself.

The final Chapter 6 is devoted to generalized Thue-Morse sequences. The classical Thue-Morse sequence, along with sturmian words, are possibly the most famous infinite words. Sturmian words can be constructed through palindromic closures, but Thue-Morse is not sturmian. However, it can be constructed using a more general variant of palindromic closure

M

(with respect to an infinite sequence of antimorphisms). Generalized Thue-Morse sequences are built using larger alphabets and digit sums (one of the classical ways of building the classical Thue-Morse). The paper succeeds on determining when a generalized Thue-Morse sequence can be built through palindromic closure in the most general sense. The necessary and sufficient condition is very simple and this beautiful theorem cannot leave indifferent anyone interested in infinite words.

The results presented in this thesis raise a number of interesting questions, many of them of speculative nature. I would like to include two in this report:

1. In the first paper, condition (C1) is very weak, it can be given by any recursive language. In Construction 1, one replaces a lobe by a Schützenberger graph, but if this graph is infinite and all we control is the word problem, is this enough? The same doubt arises at the last paragraph of page 18.

2. Has Tatiana ever considered applying combinatorial inverse semigroup theory to cryptography problems? This is being done more and more for combinatorial group theory.

As my general appreciation, I must say that this thesis demonstrates the quality of Tatiana Jajcayová's work, her maturity as a researcher and the broad scope of her interests. In particular, her articles on Schützenberger graphs of inverse semigroup presentations constitute landmarks of the theory and have earned her international recognition in the area.

The thesis is globally well written. There are a few occasional distractions, but Tatiana succeeds on giving excellent explanations for subjects which are sometimes of high technical difficulty. The thesis is a sample of her rich and diversified research activity.

For all these reasons, I strongly recommend the title of *Docent* to be awarded to Tatiana Jajcayová.

Porto, the 3rd May 2017

Pedro V. Silva

Full Professor
Department of Mathematics
Faculty of Sciences
University of Porto