Abstract of PhD Thesis

Author: Radu-Florian Atanasiu

Title: Parikh Matrix Mapping and Applications
Language: English

Supervisor: Toader Jucan
Institute: Al.I.Cuza University of Iaşi, Romania

Date: 25 June 2010

Abstract

The central notion of this thesis is the Parikh matrix mapping. Our work revolves around a critical property of the *Parikh matrix mapping*, namely the injectivity. The fact that the *Parikh matrix mapping* is not always injective has been noticed since the introduction of this extension of the classical Parikh mapping. Some of the carried out investigations explored the cases when the mapping is injective, while others characterized the words having the same image through the mapping, that is the same *Parikh matrix* (it is said about such words that they are *amiable* or *M-equivalent*). The study over the injectivity also touched other areas, such as languages. It is of no surprise that a natural extension of the Parikh matrix mapping over languages raised questions of classification within the already known classes (particularly, the Chomsky hierarchy). These subjects were addressed mostly by the present work, in some cases offering alternative results to the existing ones, in others bringing totally new contributions.

First, we present a series of results from the literature that are related to our matter. A selection is made, containing relevant results from each area approached by the thesis, while attempting to follow the logical path of their conception. They are sometimes annotated with personal observations, and moreover, their appearance (notations, different terms having the same meaning, descriptive exposition) is unified.

Then, we give a characterization of certain classes of *amiable* (or *M-equivalent*) words. The intention is to provide a base for extending the established characterizations given for binary and ternary alphabets to arbitrarily large ones. We also describe the behavior of palindromes in the context of amiability over binary alphabets. We also propose an algorithm for finding a common multiple for *Parikh matrices*. Translated to words, it means that for any two words, α and β, there is an amiability class where they appear as prefixes within some words of the class (there exist γ and δ such that $\gamma \sim_a \delta$ and $(\alpha\beta)/(\beta\alpha)$ is a prefix of γ/δ, respectively).

In the process of achieving this result other properties were found implying amiability for words composed solely from a subword and its mirror, arranged in different manners, depending on the size of the alphabet. Finally, this algorithm offers a generative meaning to amiability.

Next, we propose a message authentication method using the property of amiability. This application is represented by a *MAC*(Message Authentication Code), constructed through the aid of the Istrail morphism. The section aims at both offering the theoretical support – in this sense is given an algorithm for messages authentication and analyzed from several points of view, such as complexity – and the practical counterpart, taking the form of implementing and testing the algorithm.

Afterwards, we approach the study of the Parikh matrices from the perspective of formal languages. The final part of the thesis carries out an investigation over the complexity of the problem of deciding whether a given matrix is Parikh or not. The work is carried out with 4×4 matrices (corresponding to ternary alphabets), as a starting point for a subsequent generalization. It is shown that the language of all *Parikh matrices* is context-sensitive. We also give algorithms for telling if a given matrix is Parikh or not, having $NSPACE$ complexity. Unfortunately, it still cannot be specified how hard the problem is, however there is strong evidence that it is $PSPACE$-complete. Nonetheless, we present a pseudo-polynomial algorithm, thus having an efficient way of solving it if the entry is of reasonable size. We have discovered that this decidability problem is in NSPACE(n), at least for the case of 4×4 matrices, resembling the case of ternary languages.

Table of Contents

Author's correspondence address Radu-Florian Atanasiu
N.Caramfil str. 50, Bl.11A
Ap.12, Sector 1
014145 - Bucharest
Romania