MAP-I
Programa Doutoral em Informática
Automata and Applications

Unidade Curricular em Teoria e Fundamentos
Theory and Foundations
(UCTF)

DCC-DM-FCUP

May 2013

Abstract

This is a proposal for a UCTF ("Unidade Curricular em Teorias e Fundamentos") course in the context of the joint PhD program (Minho, Aveiro, Porto) in Informatics (Map-I). The members of the team responsible for the proposal are lecturers from the Computer Science Department and the Mathematics Department, Faculty of Science of the University of Porto.

1 Lecturing Team

Sabine Broda, António Machiavelo, Nelma Moreira, Rogério Reis

2 Course Description

2.1 Subject and Context

Automata theory (AT) is one of the foundations of Computer Science and its applications extend to several areas of computer science. Among other recent areas of application of on operations and conversions between equivalent language representations and their succinctness; descriptional complexity issues; and introduction to average case complexity. We also introduce weighted automata and transducers, and see how the standard finite automata algorithms are adapted.

The second part considers automata over infinite words and trees and briefly presents the main results about conversions and decidability problems, and its relation with logics.

The third part focuses on some recent applications of automata-theoretical approaches in four different areas. Since the seminal Büchi theorem relating finite automata with monadic second order logic, automata have been successfully applied in many different logical contexts and specially with modal and temporal logics. These logics are particularly adequate for automatic verification of reactive systems. Weighted automata approaches were successfully applied in speech recognition and image processing to deal with probabilistic reasoning. Tree automata and finite automata are the theoretical bases for XML technologies such as schema, transformations and query languages. Due to their succinctness and decidability, finite automata have several applications to security protocols and cryptography.

Finally in the fourth part we introduce cellular automata which are a class of spatially and temporally discrete mathematical systems characterized by local interaction and synchronous dynamical evolution. In the 1990's cellular automata were proposed for modeling cryptographic systems and that will be the main application we will focus on.

ACM Computing Classification System subjects covered:

- /Theory of Computation/COMPUTATION BY ABSTRACT DEVICES/Models of Computation/
- /Theory of Computation/COMPUTATION BY ABSTRACT DEVICES/Complexity Measures and Classes/
- /Theory of Computation/MATHEMATICAL LOGIC AND FORMAL LANGUAGES/
- /Theory of Computation/DISCRETE MATHEMATICS/Combinatorics/

Similar courses There are several international institutions which provide courses on the topics cover by this course. One degree were there is a specialization in these topics is the Parisian Master of Research in Computer Science (MPRI) (`https://wikimpri.dptinfo.ens-cachan.fr/doku.phpMRPI`).

2.2 Objectives

This UCTF aims

- to present some recent research work in descriptional complexity of regular languages and to consider some open problems.
- to present some other automata models and see how the classical theory extends to them.

- to present recent applications of automata theory to other computer science areas, such as specification and verification of reactive systems, cryptography, XML processing, computational linguistics, etc.

2.3 Learning Outcomes

- To understand the several representations for regular languages and operations, and their relative descriptional and computational complexity.
- To understand the several types of automata (alternating, weighted, timed, Büchi, over trees,etc) and how known algorithms for finite autmata can be adapted.
- To understand the basic concepts of transducers and their applications.
- To understand the use of generating functions and analytic combinatorics for studying average-case analysis.
- To understand the several connections between logics and automata, specially monadic, temporal and modal logics.
- To understand the diversity of applications of automata and the gain of having common algorithms to apply to very different areas.
- To understand the importance and elegance of cellular automata as models of computation for discrete systems.

2.4 Syllabus

- Part I: Automata on finite words (10h)
    1. Regular languages and their representations: regular expressions, deterministic finite automata (DFA), non-deterministic finite automata (NFA)
    2. Descriptional measures and operational complexities
    3. Enumeration and random generation of some classes of FAs
    4. Conversions between equivalent language representations and their succinctness
    5. Introduction to average case complexity based on analytic combinatorics: generating functions and analytic functions
    6. Alternating automata
    7. Weighted automata (automata with multiplicities)
    8. Transducers
- Part II: Automata on infinite words and trees (4h)

1. Büchi and Müller automata
2. Alternating automata
3. Timed automata
4. Tree automata
5. Automata and monadic logics

- Part III: Applications (8h)
  1. Verification of reactive and hybrid systems
     (a) Temporal logics
     (b) Automata-theoretic approach to decidability
     (c) Model checking
  2. XML processing
     (a) Tree languages and schema
     (b) XML language containment
  3. Speech recognition and image processing
     (a) Weighted transducers
     (b) Weighted automata for image compression
  4. Security and Cryptography
     (a) Verification of security protocols
     (b) Finite automata and public-key cryptopgraphy

- Part IV: Cellular Automata (6h)
  1. One-dimensional cellular automata (CA)
  2. Classes of CA
  3. Two-dimensional CA
  4. Universal computation in CA and complexity
  5. Applications

2.5 Student Assessment

- Examinations
- Research assignments, which may include a talk given on a suggested paper, or practical assignments

2.6 Recommended Bibliography

References

[DKV09] Manfred Droste, Werner Kuich, and Heiko Vogler, editors. *Handbook of Weighted Automata*. Monographs In Theoretical Computer Science. An Eatcs Series. Springer, 2009.

[DS12] Deepak D'Souza and Priti Shankar, editors. *Modern Applications of Automata Theory*. Iisc Research Monographs Series. World Scientific, 2012.

[EMVM06] Z. Esik, C. Martín-Vide, and V. Mitrana, editors. *Recent Advances in Formal Languages and Appplications*. Springer-Verlag, 2006.

[GTW02] E. Grädel, W. Thomas, and T. Wilke, editors. *Automata, Logics, and Infinite Games*. Springer-Verlag, 2002.

[HK11] Markus Holzer and Martin Kutrib. *Scientific Applications of Language Methods*, chapter Descriptional Complexity — An Introductory Survey, pages 1–58. Mathematics, Computing, Language, and Life: Frontiers in Mathematical Linguistics and Language Theory. Imperial College Press, carlos martín-vide edition, 2011.

[Ila01] Andrew Ilachinski. *Cellular Automata: a Discrete Universe*. World Scientific, 2001.

[KN01] B. Khoussainov and Anil Nerode. *Automata Theory and its Applications*. BirkhÄuser, 2001.

[RS97] Grzegorz Rozenberg and Arto Salomaa, editors. *Handbook of FOrmal LAnguages*. Springer, 1997.

[Sak09] Jacques Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009.

[Sha08] Jeffrey Shallit. *A Second Course in Formal Languages and Automata Theory*. Cambridge University Press, 2008.

[Wan12] Jiacun Wang, editor. *Handbook of Finite State Based Models and Applications*. Discrete Mathematics And Its Applications. Chapman And Hall/Crc Press, 2012.

3 Lecturing Team

The proponents of this course have worked actively in the past few years, on topics that are directly related to the subjects covered by this course, as detailed below.

In the context of this course, we also would like to have the opportunity to invite internationally recognized researchers such as Martin Kutrib (Universität Giessen, Germany, main research on descriptional complexity of formal languages and cellular automata), Klaus Sutner (Carnegie Mellon University, USA, works on computability and cellular automata), Jacques Sakarovitch (ENST, Paris, one of his topics of research is automata with multiplicities) or Alexandra Silva (Radboud University Nijmegen, one of her topics of research is coalgebraic methods for automata).

For this edition the coordenator will be Rogério Reis.

- Sabine Broda, has worked on Mathematical Logic. Her current research interests include automata theory and formal languages; descriptional complexity; and formal verification. She has been publishing (as well as refereeing) regularly in international journals and conferences on these areas.

- António Machiavelo has worked in Number Theory, Cryptography and Finite Automata Theory, having published a few papers on each of these subjects, namely on reversibility of cellular automata and average-case complexity based on analytic combinatorics.

- Nelma Moreira has worked in Automata Theory, Modal Logics, Verification and Logic Programming. She has several publications on international journals and conferences concerning descriptional complexity of regular languages, succinct conversions between equivalent models of regular languages and, average-case complexity based on analytic combinatorics. She has been member of program committees of several international conferences. In 2012 she was co-chair of program and organizing committees of the International Workshop Descriptional Complexity of Formal Systems (DCFS) and the International Conference on Implementation and Applications of Automata (CIAA).

- Rogério Reis, Phd in Automata Theory, his main research interests are in the area of formal languages and automata theory; descriptional complexity; enumerative and analytic combinatorics; and cryptography. He has several scientific publications in international journals and conferences. He has been member of program committees of several international conferences. In 2012 he was co-chair of program and organizing committees of the International Workshop Descriptional Complexity of Formal Systems (DCFS) and the International Conference on Implementation and Applications of Automata (CIAA). He is co-chair of the program committee of DCFS 2013.

The proponents are team members of the project CANTE (Descriptional and computational complexity of formal languages, PTDC/EIA-CCO/101904/2008) 2010-2013

which aims to obtain new, concrete characterizations of formal language representations, both from the descriptional as well as computational complexity perspective, leading to efficient manipulation methods with application to the construction of automata based certificates of program properties, and algebraic and coalgebraic methods for proof systems based in Kleene algebras. Some of them were also team members of the project RESCUE (*Reliable and Safe Code Execution for Embedded Systems*), FCT/ PTDC/ EIA/ 65862/ 2006), where they aimed to apply automata-theoretical techniques to verification in the context of PPC (Proof-Carry Code) and of the project ASA (*Automata, Semigroups and Applications*, FCT/PTDC/MAT/65481/2006) which aimed to contribute to the development of the theories of automata and semigroups, and some of their applications.