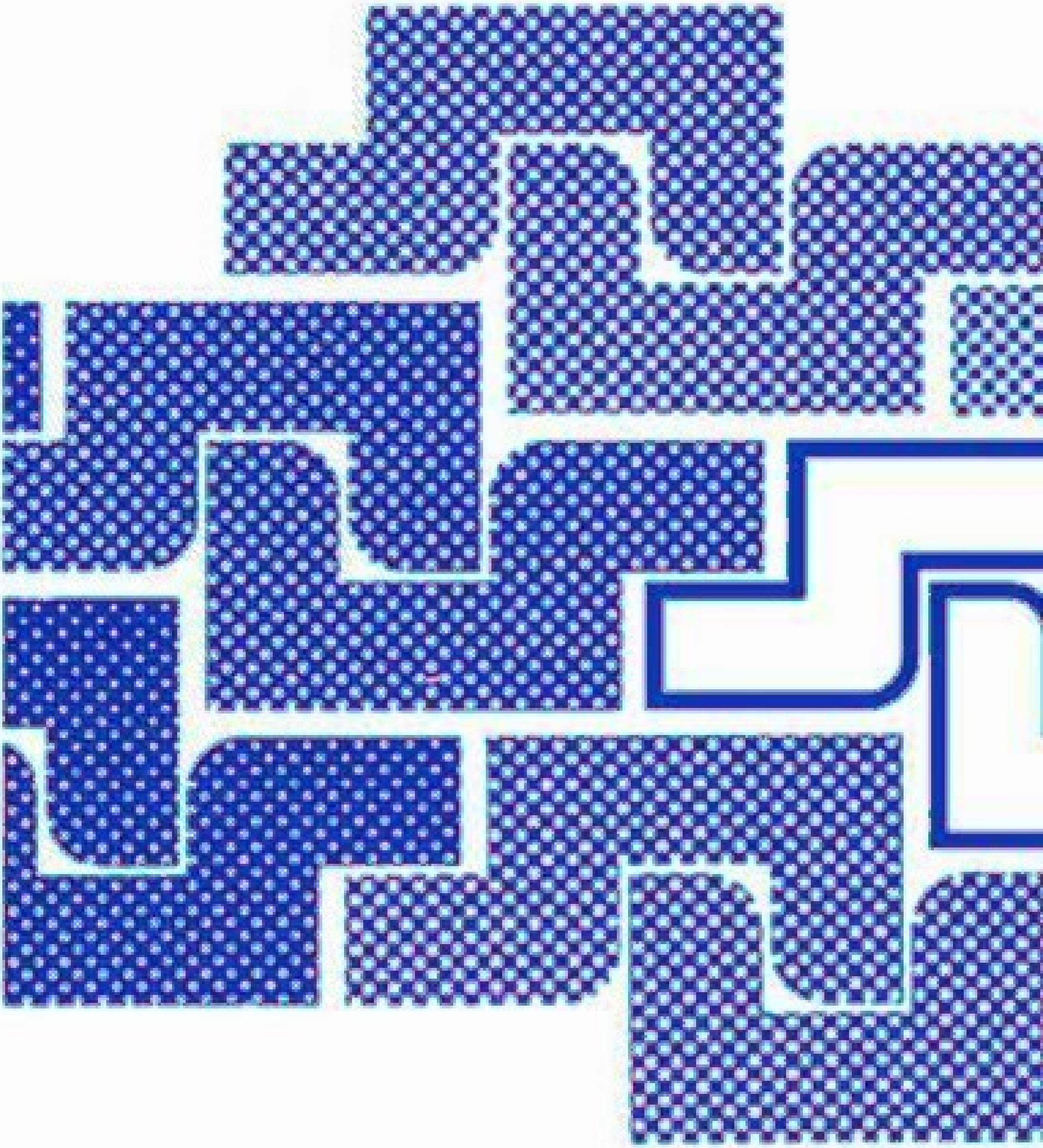


Structural Theory of Automata, Semigroups, and Universal Algebra

NATO Science Series

A Series presenting the results of scientific meetings supported under the NATO Science Programme.

The Series is published by IOS Press, Amsterdam, and Springer (formerly Kluwer Academic Publishers) in conjunction with the NATO Public Diplomacy Division.

Sub-Series

I. Life and Behavioural Sciences	IOS Press
II. Mathematics, Physics and Chemistry	Springer (formerly Kluwer Academic Publishers)
III. Computer and Systems Science	IOS Press
IV. Earth and Environmental Sciences	Springer (formerly Kluwer Academic Publishers)

The NATO Science Series continues the series of books published formerly as the NATO ASI Series.

The NATO Science Programme offers support for collaboration in civil science between scientists of countries of the Euro-Atlantic Partnership Council. The types of scientific meeting generally supported are "Advanced Study Institutes" and "Advanced Research Workshops", and the NATO Science Series collects together the results of these meetings. The meetings are co-organized by scientists from NATO countries and scientists from NATO's Partner countries — countries of the CIS and Central and Eastern Europe.

Advanced Study Institutes are high-level tutorial courses offering in-depth study of latest advances in a field.
Advanced Research Workshops are expert meetings aimed at critical assessment of a field, and identification of directions for future action.

As a consequence of the restructuring of the NATO Science Programme in 1999, the NATO Science Series was re-organized to the four sub-series noted above. Please consult the following web sites for information on previous volumes published in the Series.

http://www.nato.int/science
http://www.springeronline.com
http://www.iospress.nl

Series II: Mathematics, Physics and Chemistry – Vol. 207

Structural Theory of Automata, Semigroups, and Universal Algebra

edited by

Valery B. Kudryavtsev

Department of Mathematical Theory of Intelligent Systems,
Faculty of Mechanics and Mathematics,
M.V. Lomonosov Moscow State University,
Moscow, Russia

and

Ivo G. Rosenberg

University of Montreal,
Quebec, Canada

Technical Editor:

Martin Goldstein

Department of Mathematics and Statistics,
University of Montreal,
Quebec, Canada

Springer

Published in cooperation with NATO Public Diplomacy Division

Proceedings of the NATO Advanced Study Institute on
Structural Theory of Automata, Semigroups and Universal Algebra
Montreal, Quebec, Canada
7–18 July 2003

A C.I.P. Catalogue record for this book is available from the Library of Congress.

ISBN-10 1-4020-3816-X (PB)
ISBN-13 978-1-4020-3816-7 (PB)
ISBN-10 1-4020-3815-1 (HB)
ISBN-13 978-1-4020-3815-0 (HB)
ISBN-10 1-4020-3817-8 (e-book)
ISBN-13 978-1-4020-3817-4 (e-book)

Published by Springer,
P.O. Box 17, 3300 AA Dordrecht, The Netherlands.

www.springeronline.com

Printed on acid-free paper

Printed in the Netherlands.

Table of Contents

Preface

In the summer of 2003 the Department of Mathematics and Statistics of the University of Montreal was fortunate to host the NATO Advanced Study Institute "Structural theory of Automata, Semigroups and Universal Algebra" as its 42nd Séminaire des mathématiques supérieures (SMS), a summer school with a long tradition and well-established reputation. This book contains the contributions of most of its invited speakers.

It may seem that the three disciplines in the title of the summer school cover too wide an area while its three parts have little in common. However, there was a high and surprising degree of coherence among the talks. Semigroups, algebras with a single associative binary operation, is probably the most mature of the three disciplines with deep results. Universal Algebra treats algebras with several operations, e.g., groups, rings, lattices and other classes of known algebras, and it has borrowed from formal logics and the results of various classes of concrete algebras. The Theory of Automata is the youngest of the three. The Structural Theory of Automata essentially studies the composition of small automata to form larger ones. The role of semigroups in automata theory has been recognized for a long time but conversly automata have also influenced semigroups. This book demonstrates the use of universal algebra concepts and techniques in the structural theory of automata as well as the reverse influences.

J. Almeida surveys the theory of profinite semigroups which grew from finite semigroups and certain problems in automata. There arises a natural algebraic structure with an interplay between topological and algebraic aspects. Pseudovarieties connect profinite semigroups to universal algebras. L. N. Shevrin surveys the very large and substantial class of special semigroups, called epigroups. He presents them as semigroups with the unary operator of pseudo-inverse and studies some nice decompositions and finiteness conditions.

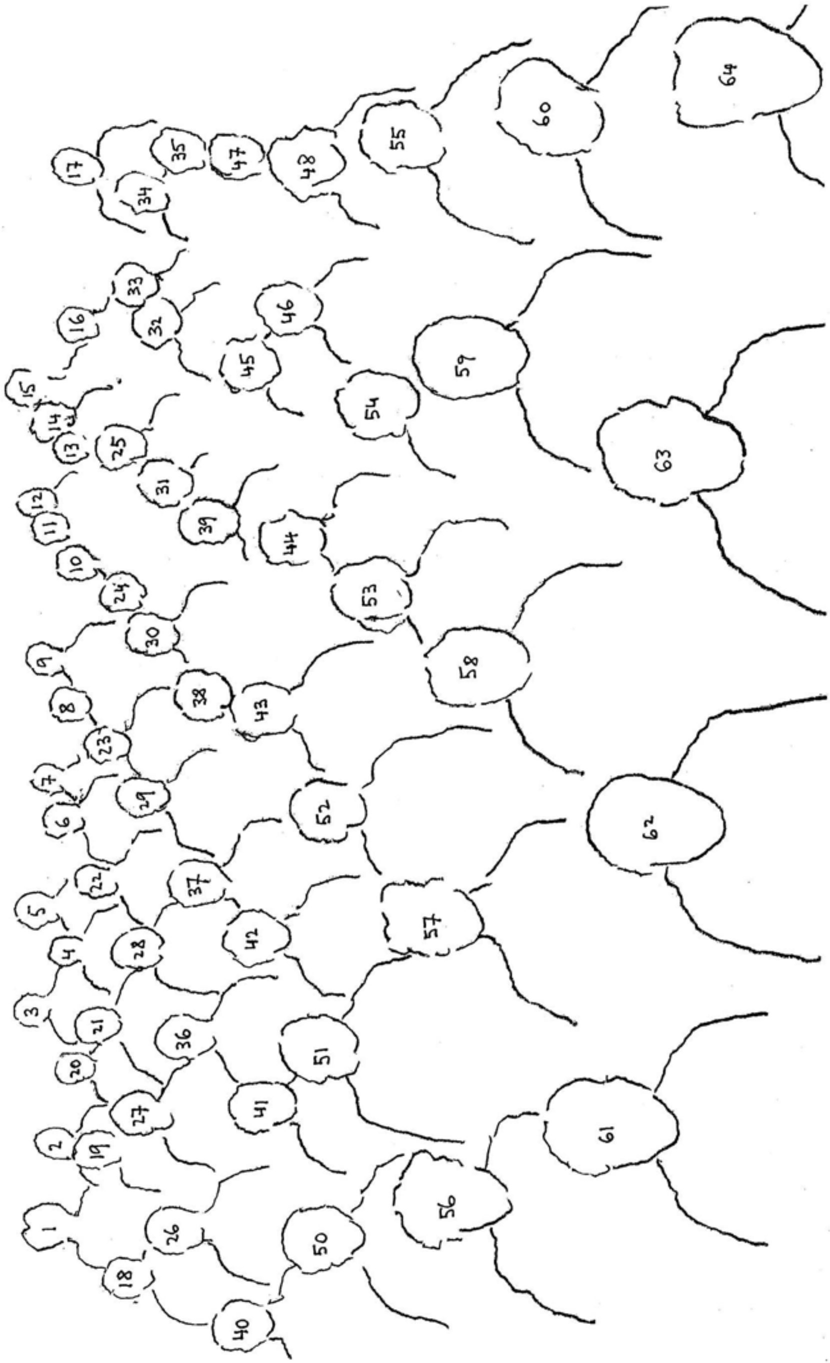
A. Letichevsky studies transition systems, an extension of automata, behaviour algebras and other structures. He develops a multifaceted theory of transition systems with many aspects. J. Dassow studies various completeness results for the algebra of sequential functions on $\{0, 1\}$, essentially functions induced by automata or logical nets. In particular, he investigates completeness with respect to an equivalence relation on the algebra. V. B. Kudryavtsev surveys various completeness and expressibility problems and results starting from the completeness (primality) criterion in the propositional calculus of many-valued logics (finite algebras) to delayed algebras and automata functions. T. Hikita and I. G. Rosenberg study the week completeness of finite delayed algebras situated between universal algebras and automata. The relational counterpart of delayed clones is based on infinite sequences of relations. All the corresponding maximal clones are described except for those determined by sequences of equivalence relations or by sequences of binary central relations.

In the field of Universal Algebra J. Berman surveys selected results on the structure of free algebraic systems. His focus is on decompositions of free algebras into simpler components whose interactions can be readily determined. P. Idziak studies the G-spectrum of a variety, a sequence whose k-th term is the number of k-generated algebras in the variety. Based on commutator and tame congruence theory the at most polynomial and at most exponential G-spectra of some locally finite varieties are described. M. Jackson studies the syntactic semigroups. He shows how to efficiently associate a syntactic semigroup (monoid) with a finite set of identities to a semigroup (monoid) with a finite base of identities and finds a language-theoretic equivalent of the above finite basis problem. K. Kaarli and L. Márki survey endoprimal algebras, i.e. algebras whose term operations comprise all operations admitting a given monoid of selfmaps as their endomorphism monoid. First they present the connection to algebraic dualisability and then characterize the endoprimal algebras among Stone algebras, Kleene algebras, abelian groups, vector spaces, semilattices and implication algebras. A. Krokhin, A. Bulatov and P. Jevons investigate the constraint satisfaction problem arising in artificial intelligence, databases and combinatorial optimization. The algebraic counterpart of this relational problem is a problem in clone theory. The paper studies the computational complexity aspects of the constraint satisfaction problem in clone terms. R. McKenzie and J. Snow present the basic theory of commutators in congruence modular varieties of algebras, an impressive machinery for attacking diverse problems in congruence modular varieties.

It is fair to state that we have met our objective of bringing together specialists and ideas in three neighbouring and closely interrelated domains. To all who helped to make this SMS a success, lecturers and participants alike, we wish to express our sincere thanks and appreciation. Special thanks go to Professor Gert Sabidussi for his experience, help and tireless efforts in the preparation and running of the SMS and, in particular, to Ghislaine David, its very efficient and charming secretary, for the high quality and smoothness with which she handled the organization of the meeting. We also thank Professor Martin Goldstein for the technical edition of this volume.

Funding for the SMS was provided in the largest part by NATO ASI Program with additional support from the Centre de recherches mathématiques of the Université de Montréal and from the Université de Montréal. To all three organizations we would like to express our gratitude for their support.

Ivo G. Rosenberg


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64

Key to group picture

1 Hartmann
2 Kun
3 Dinu
4 Vertesi
5 McNulty
6 Salehi
7 Vernikov
8 Piirainen
9 Semigrodskikh
10 Descalço
11 Kudryavtseva
12 Ferreira
13 Silva
14 Maroti
15 Gouveia da Costa
16 F. Almeida
17 Idziak
18 Kaarli
19 Kühr
20 Magnifo Kahou
21 Kuchmei
22 Snow
23 Jackson
24 Kambites
25 Kirsten
26
27 Rachunek
28 Márki
29
30 Halas
31 Ondrusch
32 Kufleitner
33 Mäurer
34 Püschmann
35 Gorachinova
36 Vladislavlev
37 Galatenko
38 Uvarov
39
40 Seif
41 Legault
42 J.-L. David
43 Szabó
44 Chajda
45 Fleischer
46 Sezinando
47 Fearnley
48 Gomes
49 J. Almeida
50 Haddad
51
52 Hikita
53 G. David
54 Sabidussi
55 Dassow
56 McKenzie
57 Krokhin
58 Volkov

59 Shevrin
60 Letichevsky
61 Berman
62 Freivalds
63 Steinby
64 Rosenberg

Participants

Filipa ALMEIDA
Centro de Álgebra
Universidade de Lisboa
Av. Prof. Gama Pinto, 2
P-1649-003 Lisboa
Portugal
filipasda@hotmail.com

Sergiy BORODAY
Centre de recherche informatique de Montréal
550, rue Sherbrooke O. bureau 100
Montréal, QC H3A 1B9
Canada
sboroday@crim.ca

Ivan CHAJDA
Department of Algebra and Geometry
Palacky University, Olomouc
Tomkova 40
779 00 Olomouc
Czech Republic
chajda@risc.upol.cz

Luis A. A. DESCALÇO
Departamento de Matemática
Universidade de Aveiro
P-3810-193 Aveiro
Portugal
luisd@mat.ua.pt

Petrisor Liviu DINU
Faculty of Mathematics
University of Bucharest
14 Academiei St.
70190 Bucharest
Romania
ldinu@funinf.cs.unibuc.ro

Anne FEARNLEY
Dép. de mathématiques et de statistique
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
fearnley@dms.umontreal.ca

Marco A. Semana FERREIRA
Escola Superior de Tecnologia de Viseu
Campus Politécnico de Repeses
P-3504-510 Viseu
Portugal
mferreira@math.estv.ipv.pt

Isidore FLEISCHER
Centre de recherches mathématiques
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
fleischi@crm.umontreal.ca

Rusins FREIVALDS
Inst. of Mathematics and Computer Science
University of Latvia
Raina bulvaris 29
Riga, LV-1459
Latvia
rusins.freivalds@mii.lu.lv

Alexei GALATENKO
Department of MaTIS
Moscow State University
Vorobjevy Gory
119899 Moscow
Russia
agalat@msu.ru

Igor GOLDBERG
Department of Mathematics and Mechanics
Ural State University
Pr. Lenina 51
620083 Ekaterinbourg
Russia
goldberg@skbkontur.ru

Gracinda M. GOMES
Centro de Álgebra
Universidade de Lisboa
Av. Prof. Gama Pinto, 2
P-1649-003 Lisboa
Portugal
ggomes@cii.fc.ul.pt

Lidja GORACHINOVA-ILIEVA
Pedagogical Faculty "Gotse Delchev"
G. Delchev 89
2000 Shtip
Macedonia
fildim@mt.net.mk

Nicolas GORSE
Département d'informatique
et de recherche opérationnelle
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
gorsen@iro.umontreal.ca

Alfredo GOUVEIA DA COSTA
Departamento de Matemática
Universidade de Coimbra
Apartado 3008
P-3001-454 Coimbra
Portugal
amgcd@mat.uc.pt

Vera GROUNSKAIA
Ul'yanovsk State University
Dimitrova 4
433507 Ul'yanovskaya obl.
Dimitrovgrad
Russia
grunska@vinf.ru

Lucien HADDAD
Dept. of Mathematics and Computer Science
Royal Military College of Canada
P.O. Box 17000 Station Forces
Kingston, ON K7K 7B4
Canada
haddad-l@rmc.ca

Radomir HALAS
Department of Algebra and Geometry
Palacky University, Olomouc
Tomkova 40
779 00 Olomouc
Czech Republic
halas@risc.upol.cz

Miklós HARTMANN
Bolyai Institute
University of Szeged
Aradi vértanúk tere 1
6720 Szeged
Hungary
mota@petra.hos.u-szeged.hu

Mark KAMBITES
Department of Mathematics
University of York
Heslington
York YO10 5DD
UK
mek100@york.ac.uk

Christopher KERMOVANT
Département d'informatique
et de recherche opérationnelle
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada

Daniel KIRSTEN
LIAFA
Université Paris 7
Case 7014
Place Jussieu
F-75251 Paris Cedex 05
France
kirsten@liafa.jussieu.fr

Vladimir KUCHMEI
Institute of Pure Mathematics
Fac. of Mathematics and Computer Science
University of Tartu
J. Liivi 2-218
Estonia
kucmei@math.ut.ee

Ganna KUDRYAVTSEVA
Faculty of Mechanics and Mathematics
National Taras Shevchenko University of Kiev
64 Volodymyrs'ka St.
01033 Kiev
Ukraine
anjaua@yahoo.com

Manfred KUFLEITNER
Institut für Formale Methoden der Informatik
University of Stuttgart
Universitätsstraße 38
D-70569 Stuttgart
Germany
manfred.kufleitner@informatik.uni-stuttgart.de

Jan KÜHR
Department of Algebra and Geometry
Palacky University, Olomouc
Tomkova 40
779 00 Olomouc
Czech Republic
kuhr@inf.upol.cz

Gabor KUN
Department of Algebra and Number Theory
Eötvös University
Pázmány Péter sétény 1/c.
H-1117 Budapest
Hungary
kungabor@cs.elte.hu

Éric LACOURSIÈRE
Dép. d'informatique et de génie logiciel
Université Laval
Québec, QC G1K 7P4
Canada
eric.lacoursiere@ift.ulaval.ca

Florence Laure MAGNIFO KAHOU
Dép. de mathématiques et de statistique
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
magnifo@dms.umontreal.ca

Miklos MAROTI
Institute for Software Integrated Systems
Vanderbilt University
Box 1829, Station B
Nashville, TN 37235
USA
mmaroti@math.vanderbilt.edu

Ina MÄURER
Institut für Algebra
Technische Universität Dresden
01062 Dresden
Germany
maeurer@math.tu-dresden.de

Pierre MCKENZIE
Département d'informatique
et de recherche opérationnelle
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
mckenzie@iro.umontreal.ca

George MCNULTY
Department of Mathematics
University of South Carolina
1523 Greene Str.
Columbia, SC 29208
USA
mcnulty@math.sc.edu

Nicole ONDRUSCH
Institut für Formale Methoden der Informatik
University of Stuttgart
Universitätsstraße 38
D-70569 Stuttgart
Germany
ondrusch@informatik.uni-stuttgart.de

Ville PIIRAINEN
Turku Centre for Computer Science
Lemminkäisenkatu 14 A, 5th floor
FIN-20520 Turku
Finland
ville.piirainen@utu.fi

Simon PILETTE
Département d'informatique
et de recherche opérationnelle
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
simon.pilette@umontreal.ca

Svetlana PLESCHEVA
Department of Mathematics and Mechanics
Ural State University
Pr. Lenina 51
620083 Ekaterinbourg
Russia
plescheva81@mail.ru

Ulrike PÜSCHMANN
Institut für Algebra
Technische Universität Dresden
01062 Dresden
Germany
u.pueschmann@gmx.net

Jiri RACHUNEK
Department of Algebra and Geometry
Palacky University, Olomouc
Tomkova 40
779 00 Olomouc
Czech Republic
rachunek@risc.upol.cz

Gert SABIDUSSI
Dép. de mathématiques et de statistique
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
sab@dms.umontreal.ca

Saeed SALEHIPOURMEHR
Turku Centre for Computer Science
Lemminkäisenkatu 14 A, 5th floor
FIN-20520 Turku
Finland
saeed@cs.utu.fi

Steve R. SEIF
Department of Mathematics
University of Louisville
Louisville, KY 40292
USA
swseif@louisville.edu

Victor SELIVANOV
Department of Computer Science
Novosibirsk State Pedagogical University
Viluiskaya 28
630126 Novosibirsk
Russia
vseliv@nspu.ru

Alexander SEMIGRODSKIKH
Department of Mathematics and Mechanics
Ural State University
Pr. Lenina 51
620083 Ekaterinbourg
Russia
alexander.semigrodskikh@usu.ru

Helena SEZINANDO
Departamento de Matemática
Universidade de Lisboa
Rua E. de Vasconcelos Bl. C, piso 13
P-1749-016 Lisboa
Portugal
mhelena@ptmat.fc.ul.pt

Nelson SILVA
School of Mathematics and Statistics
University of St Andrews
North Haugh
Fife KY16 9SS
UK
nelson@mcs.st-and.ac.uk

Csaba SZABÓ
Department of Algebra and Number Theory
Eötvös University
Pázmány Péter sétény 1/c.
H-1117 Budapest
Hungary
csaba@cs.elte.hu

Dmitri UVAROV
Department of MaTIS
Moscow State University
Vorobjevy Gory
119899 Moscow
Russia
dima@uvarov.ru

Matt VALERIOTE
Department of Mathematics and Statistics
McMaster University
1280 Main St. West
Hamilton, Ontario L8S 4K1
Canada
matt@math.mcmaster.ca

Victor VLADISLAVLEV
Faculty of Mechanics and Mathematics
Moscow State University
Vorobjevy Gory
119899 Moscow
Russia
vladisla@mcst.ru

Boris M. VERNIKOV
Department of Mathematics and Mechanics
Ural State University
Pr. Lenina 51
620083 Ekaterinbourg
Russia
boris.vernikov@usu.ru

Mikhail VOLKOV
Department of Mathematics and Mechanics
Ural State University
Pr. Lenina 51
620083 Ekaterinbourg
Russia
mikhail.volkov@usu.ru

Vera VERTESI
Department of Algebra and Number Theory
Eötvös University
Pázmány Péter sétény 1/c.
H-1117 Budapest
Hungary
wera13@cs.elte.hu

Contributors

Jorge ALMEIDA
Departamento de Matemática Pura
Universidade do Porto
Rua do Campo Alegre, 687
4169-007 Porto
Portugal
jalmeida@fc.up.pt

Joel BERMAN
Department of Mathematics, Statistics and Computer Science
University of Illinois at Chicago
851 South Morgan
Chicago, IL 60607
USA
jberman@uic.edu

Andrei BULATOV
School of Computer Science
Simon Fraser University
Burnaby, BC V5A 1S6
Canada

Jürgen DASSOW
Fakultät für Informatik
Otto-von-Guericke-Universität
PSF 4120
D-39016 Magdeburg
Germany
dassow@iws.cs.uni-magdeburg.de

Teruo HIKITA
Department of Computer Science
Meiji University
1-1-1 Higashimita
Tama-ku, Kawasaki 214-8571
Japan
hikita@cs.meiji.ac.jp

Paweł M. IDZIAK
Computer Science Department
Jagiellonian University
Nawojki 11
PL-30-072 Kraków
Poland
idziak@ii.uj.edu.pl

Marcel JACKSON
Department of Mathematics
La Trobe University
3086 Victoria
Australia
m.g.jackson@latrobe.edu.au

Peter JEAVONS
Computing Laboratory
University of Oxford
Oxford OX1 3QD
UK

Kalle KAARLI
Institute of Pure Mathematics
University of Tartu
50090 Tartu
Estonia
kaarli@math.ut.ee

László MÁRKI
A. Rényi Institute of Mathematics
Hungarian Academy of Sciences
Pf. 127
H-1364 Budapest
Hungary
marki@renyi.hu

Andrei KROKHIN
Department of Computer Science
University of Durham
Durham, DH1 3LE
UK
andrei.krokhin@durham.ac.uk

Valery B. KUDRYAVTSEV
Department of MaTIS
Moscow State University
Vorobjevy Gory
119899 Moscow
Russia
kudryavtsev@lsili.ru

Alexander LETICHEVSKY
Glushkov Institute of Cybernetics
National Academy of Sciences of Ukraine
252601 Kiev
Ukraine
al@letichevsky.kiev.ua

Ralph MCKENZIE
Department of Mathematics
Vanderbilt University
Nashville, TN 37240
USA
mckenzie@math.vanderbilt.edu

Ivo G. ROSENBERG
Dép. de mathématiques et de statistique
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, QC H3C 3J7
Canada
rosenb@dms.umontreal.ca

Lev N. SHEVRIN
Department of Mathematics and Mechanics
Ural State University
Lenina 51
620083 Ekaterinburg
Russia
Lev.Shevrin@usu.ru

John SNOW
Department of Mathematics
Concordia University
Seward, NE 68434
USA
john.snow@cune.org

Magnus STEINBY
Department of Mathematics
University of Turku
FIN-20014 Turku
Finland
steinby@utu.fi

Profinite semigroups and applications

Jorge ALMEIDA

Departamento de Matemática Pura, Faculdade de Ciências
Universidade do Porto
Rua do Campo Alegre, 687, 4169-007 Porto
Portugal

Notes taken by Alfredo COSTA

Abstract

Profinite semigroups may be described briefly as projective limits of finite semigroups. They come about naturally by studying pseudovarieties of finite semigroups which in turn serve as a classifying tool for rational languages. Of particular relevance are relatively free profinite semigroups which for pseudovarieties play the role of free algebras in the theory of varieties. Combinatorial problems on rational languages translate into algebraic-topological problems on profinite semigroups. The aim of these lecture notes is to introduce these topics and to show how they intervene in the most recent developments in the area.

1 Introduction

With the advent of electronic computers in the 1950's, the study of simple formal models of computers such as automata was given a lot of attention. The aims were multiple: to understand the limitations of machines, to determine to what extent they might come to replace humans, and later to obtain efficient schemes to organize computations. One of the simplest models that quickly emerged is the finite automaton which, in algebraic terms, is basically the action of a finitely generated free semigroup on a finite set of states and thus leads to a finite semigroup of transformations of the states [48, 61].

In the 1960's, the connection with finite semigroups was first explored to obtain computability results [79] and in parallel a decomposition theory of finite computing devices inspired by the theory of groups and the complexity of such decompositions [51, 52], again led to the development of a theory of finite semigroups [21], which had not previously merited any specific attention from specialists on semigroups.

In the early 1970's, both trends, the former more combinatorial and more directly concerned with applications in computer science, the latter more algebraic, continued to flourish with various results that nowadays are seen as pioneering. In the mid-1970's, S. Eilenberg, in part with the collaboration of M. P. Schützenberger and B. Tilson [35, 36] laid the foundations for a theory which was already giving signs of being potentially quite rich. One of the cornerstones of their work is the notion of a pseudovariety of semigroups and a correspondence between such pseudovarieties and varieties of rational languages which provided a systematic framework and a program for the classification of rational languages.

V. B. Kudryavtsev and I. G. Rosenberg (eds.),
Structural Theory of Automata, Semigroups, and Universal Algebra, 1–45.

The next ten years or so were rich in the execution of Eilenberg's program [53, 64, 65] which in turn led to deep problems such as the identification of the levels of J. Brzozowski's concatenation hierarchy of star-free languages [29] while various steps forward were taken in the understanding of the Krohn-Rhodes group complexity of finite semigroups [73, 71, 47].

In the beginning of the 1980's, the author was exploring connections of the theory of pseudovarieties with Universal Algebra to obtain information on the lattice of pseudovarieties of semigroups and to compute some operators on pseudovarieties (see [3] for results and references). The heart of the combinatorial work was done by manipulating identities and so when J. Reiterman [70] showed that it was possible to define pseudovarieties by pseudoidentities, which are identities with an enlarged signature whose interpretation in finite semigroups is natural, this immediately appeared to be a powerful tool to explore. Reiterman introduced pseudoidentities as formal equalities of implicit operations, and defined a metric structure on sets of implicit operations but no algebraic structure. There is indeed a natural algebraic structure and the interplay between topological and algebraic structure turns out to be very rich and very fruitful.

Thus, the theory of finite semigroups and applications led to the study of profinite semigroups, particularly those that are free relative to a pseudovariety. These structures play the role of free algebras for varieties in the context of profinite algebras, which already explains the interest in them. When the first concrete new applications of this approach started to appear (see [3] for results and references), other researchers started to consider it too and nowadays it is viewed as an important tool which has found applications across all aspects of the theory of pseudovarieties.

The aim of these notes is to introduce this area of research, essentially from scratch, and to survey a significant sample of the most important recent developments. In Section 2 we show how the study of finite automata and rational languages leads to study pseudovarieties of finite semigroups and monoids, including some of the key historical results.

Section 3 explains how relatively free profinite semigroups are found naturally in trying to construct free objects for pseudovarieties, which is essentially the original approach of B. Banaschewski [26] in his independent proof that pseudoidentities suffice to define pseudovarieties. The theory is based here on projective limits but there are other alternative approaches [3, 7]. Section 3 also lays the foundations of the theory of profinite semigroups which are further developed in Section 4, where the operational aspect is explored. Section 4 also includes the recent idea of using iteration of implicit operations to produce new implicit operations. Subsection 4.3 presents for the first time a proof that the monoid of continuous endomorphisms of a finitely generated profinite semigroup is profinite so that implicit operations on finite monoids also have natural interpretations in that monoid.

The remaining sections are dedicated to a reasonably broad survey, without proofs, of how the general theory introduced earlier can be used to solve problems. Section 5 sketches the proof of I. Simon's characterization of piecewise testable languages in terms of the solution of the word problem for free pro-J semigroups. Section 6 presents an introduction to the notion of tame pseudovarieties, which is a sophisticated tool to handle decidability questions which extends the approach of C. J. Ash to the "Type II conjecture" of J. Rhodes, as presented in the seminal paper [22]. The applications of this approach can be found in Sections 7 and 8 in the computation of several pseudovarieties obtained by applying natural operators to known pseudovarieties. The difficulty in this type of calculation is that it is known that those operators do not preserve decidability [1, 72, 24]. The notion of tameness came about precisely in trying to find a stronger form of decidability which would be preserved or at least guarantee decidability of the operator image [15].

Finally, Section 9 introduces some very recent developments in the investigation of connections between free profinite semigroups and Symbolic Dynamics. The idea to explore such connections eventually evolved from the need to build implicit operations through iteration in order to prove that the pseudovariety of finite p-groups is tame [6]. Once a connection with Symbolic Dynamics emerged several applications were found but only a small aspect is surveyed in Section 9, namely that which appears to have a potential to lead to applications of profinite semigroups to Symbolic Dynamics.

2 Automata and languages

An abstraction of the notion of an *automaton* is that of a semigroup S acting on a set Q, whose members are called the *states* of the automaton. The action is given by a homomorphism $\varphi : S \to \mathcal{B}_Q$ into the semigroup of all binary relations on the set Q, which we view as acting on the right. If all binary relations in $\varphi(S)$ have domain Q, then one talks about a *complete* automaton, as opposed to a *partial* automaton in the general situation. If all elements of $\varphi(S)$ are functions, then the automaton is said to be *deterministic*. The semigroup $\varphi(S)$ is called the *transition semigroup* of the automaton. In some contexts it is better to work with monoids, and then one assumes the acting semigroup S to be a monoid and the action to be given by a monoid homomorphism φ.

Usually, a set of generators A of the acting semigroup S is fixed and so the action homomorphism φ is completely determined by its restriction to A. In case both Q and A are finite sets, the automaton is said to be *finite*. Of course the restriction that Q is finite is sufficient to ensure that the transition semigroup of the automaton is finite.

To be used as a recognition device, one fixes for an automaton a set I of *initial* states and a set F of *final* states. Moreover, in Computer Science one is interested in recognizing sets of words (or strings) over an alphabet A, so that the acting semigroup is taken to be the semigroup A^+ freely generated by A, consisting of all non-empty words in the letters of the *alphabet* A. The *language recognized* by the automaton is then the following set of words:

$$L = \{w \in A^+ : \varphi(w) \cap (I \times F) \neq \emptyset\}. \tag{2.1}$$

If the empty word 1 is also relevant, then one works instead in the monoid context and one considers the free monoid A^*, the formula (2.1) for the language recognized being then suitably adapted. Whether one works with monoids or with semigroups is often just a matter of personal preference, although there are some instances in which the two theories are not identical. Most results in these notes may be formulated in both settings and we will sometimes switch from one to the other without warning. Parts of the theory may be extended to a much a more general universal algebraic context (see [3, 7] and M. Steinby's lecture notes in this volume).

For an example, consider the automaton described by Fig. 1 where we have two states, 1 and 2, the former being both initial and final, and two acting letters, a and b, the action being determined by the two partial functions associated with a and b, respectively $\bar{a} : 1 \mapsto 2$ and $\bar{b} : 2 \mapsto 1$. The language of $\{a, b\}^*$ recognized by this automaton consists of all words of the form $(ab)^k$ with $k \geq 0$ which are *labels* of paths starting and ending at state 1. This is the submonoid generated by the word ab, which is denoted $(ab)^*$.

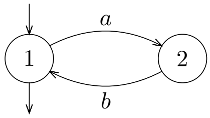


Figure 1

In terms of the action homomorphism, the language L of (2.1) is the inverse image of a specific set of binary relations on Q. We say that a language $L \subseteq A^+$ is *recognized* by a homomorphism $\psi : A^+ \to S$ into a semigroup S if there exists a subset $P \subseteq S$ such that $L = \psi^{-1}P$ or, equivalently, if $L = \psi^{-1}\psi L$. We also say that a language is *recognized* by a finite semigroup S if it is recognized by a homomorphism into S. By the very definition of recognition by a finite automaton, every language which is recognized by such a device is also recognized by a finite semigroup.

Conversely, if $L = \psi^{-1}\psi L$ for a homomorphism $\psi : A^+ \to S$ into a finite semigroup, then one can construct an automaton recognizing L as follows: for the set of states take S^1, the monoid obtained from S by adjoining an identity if S is not a monoid and S otherwise; for the action take the composition of ψ with the *right regular representation*, namely the homomorphism $\varphi : A^+ \to \mathcal{B}_{S^1}$ which sends each word w to right translation by $\psi(w)$, that is the function $s \mapsto s\psi(w)$. This proves the following theorem and, by adding the innocuous assumption that ψ is onto, it also shows that every language which is recognized by a finite automaton is also recognized by a finite complete deterministic automaton with only one initial state (the latter condition being usually taken as part of the definition of deterministic automaton).

2.1 Theorem (Myhill [61]) *A language L is recognized by a finite automaton if and only if it is recognized by a finite semigroup.*

In particular, the complement $A^+ \setminus L$ of a language $L \subseteq A^+$ recognized by a finite automaton is also recognized by a finite automaton since a homomorphism into a finite semigroup recognizing a language also recognizes its complement.

A language $L \subseteq A^*$ is said to be *rational* (or *regular*) if it may be expressed in terms of the empty language and the languages of the form $\{a\}$ with $a \in A$ by applying a finite number of times the binary operations of taking the union $L \cup K$ of two languages L and K or their concatenation $LK = \{uv : u \in L, v \in K\}$, or the unary operation of taking the submonoid L^* generated by L; such an expression is called a *rational expression* of L. For example, if letters stand for elementary tasks a computer might do, union and concatenation correspond to performing tasks respectively in parallel or in series, while the star operation corresponds to iteration. The following result makes an important connection between this combinatorial concept and finite automata. Its proof can be found in any introductory text to automata theory such as Perrin [63].

2.2 Theorem (Kleene [48]) *A language L over a finite alphabet is rational if and only if it is recognized by some finite automaton.*

An immediate corollary which is not evident from the definition is that the set of rational languages $L \subseteq A^*$ is closed under complementation and, therefore it constitutes a Boolean subalgebra of the algebra $\mathcal{P}(A^+)$ of all languages over A.

Rational languages and finite automata play a crucial role in both Computer Science and current applications of computers, since many very efficient algorithms, for instance for dealing with large texts use such entities [34]. This already suggests that studying finite semigroups should be particularly relevant for Computer Science. We present next one historical example showing how this relevance may be explored.

The *star-free* languages over an alphabet A constitute the smallest Boolean subalgebra closed under concatenation of the algebra of all languages over A which contains the empty language and the languages of the form $\{a\}$ with $a \in A$. In other words, this definition may be formulated as that of rational languages but with the star operation replaced by complementation. *Plus-free* languages $L \subseteq A^+$ are defined similarly.

On the other hand we say that a finite semigroup S is *aperiodic* if all its subsemigroups which are groups (in this context called simply *subgroups*) are trivial. Equivalently, the cyclic subgroups of S should be trivial, which translates in terms of universal laws to stating that S should satisfy some identity of the form $x^{n+1} = x^n$.

The connection between these two concepts, which at first sight have nothing to do with each other, is given by the following remarkable theorem.

2.3 Theorem (Schützenberger [79]) *A language over a finite alphabet is star-free if and only if it is recognized by a finite aperiodic monoid.*

Eilenberg [36] has given a general framework in which Schützenberger's theorem becomes an instance of a general correspondence between families of rational languages and finite monoids. To formulate this correspondence, we first introduce some important notions.

The *syntactic congruence* of a subset L of a semigroup S is the largest congruence ρ_L on S which *saturates* L in the sense that L is a union of congruence classes. The existence of such a congruence may be easily established even for arbitrary subsets of universal algebras [3, Section 3.1]. For semigroups, it is easy to see that it is the congruence ρ_L defined by $u \;\rho_L\; v$ if, for all $x, y \in S^1$, $xuy \in L$ if and only if $xvy \in L$, that is if u and v appear as factors of members of L precisely in the same context. The quotient semigroup S/ρ_L is called the *syntactic semigroup* of L and it is denoted $\operatorname{Synt} L$; the natural homomorphism $S \to S/\rho_L$ is called the *syntactic homomorphism* of L.

The syntactic semigroup $\operatorname{Synt} L$ of a rational language $L \subseteq A^+$ is the smallest semigroup S which recognizes L. Indeed all semigroups of minimum size which recognize L are isomorphic. To prove this, one notes that a homomorphism $\psi : A^+ \to S$ recognizing L may as well be taken to be onto, in which case S is determined up to isomorphism by a congruence on A^+, namely the *kernel* congruence $\ker \psi$ which identifies two words if they have the same image under ψ. The assumption that ψ recognizes L translates in terms of this congruence by stating that $\ker \psi$ saturates L and so $\ker \psi$ is contained in ρ_L. Noting that rationality really played no role in the argument, this proves the following result where we say that a semigroup S *divides* a semigroup T and we write $S \prec T$ if S is a homomorphic image of some subsemigroup of T.

2.4 Proposition *A language $L \subseteq A^+$ is recognized by a semigroup S if and only if* $\operatorname{Synt} L$ *divides S.*

The syntactic semigroup of a rational language L may be effectively computed from a rational expression for the language. Namely, one can efficiently compute the *minimal automaton* of L [63], which is the complete deterministic automaton recognizing L with the minimum number of states; the syntactic semigroup is then the transition semigroup of the minimal automaton.

Given a finite semigroup S, one may choose a finite set A and an onto homomorphism $\varphi : A^+ \to S$: for instance, one can take $A = S$ and let φ be the homomorphism which extends the identity funtion $A \to S$. For each $s \in S$, let $L_s = \varphi^{-1}s$. Since φ is an onto homomorphism which recognizes L_s, there is a homomorphism $\psi_s : S \to \operatorname{Synt} L_s$ such that the composite function $\psi_s \circ \varphi : A^+ \to \operatorname{Synt} L_s$ is the syntactic homomorphism of L_s. The functions ψ_s induce a homomorphism $\psi : S \to \prod_{s\in S} \operatorname{Synt} L_s$ which is injective since $\psi_s(t) = \psi_s(s)$ means that there exist $u, v \in A^+$ such that $\varphi(u) = s$, $\varphi(v) = t$ and $u \ \rho_{L_s} \ v$, which implies that $v \in L_s$ since $u \in L_s$ and so $t = s$. As we did at the beginning of the section, we may turn $\varphi : A^+ \to S$ into an automaton which recognizes each of the languages L_s and from this any proof of Kleene's Theorem will yield a rational expression for each L_s. Hence we have the following result.

2.5 Proposition *For every finite semigroup S one may effectively compute rational languages $L_1, \dots, L_n$ over a finite alphabet A which are recognized by S and such that S divides $\prod_{i=1}^n \operatorname{Synt} L_i$.*

It turns out there are far too many finite semigroups for a classification up to isomorphism to be envisaged [78]. Instead, from the work of Schützenberger and Eilenberg eventually emerged [36, 37] the classification of classes of finite semigroups called *pseudovarieties.* These are the (non-empty) closure classes for the three natural algebraic operators in this context, namely taking homomorphic images, subsemigroups and finite direct products. For example, the classes A, of all finite aperiodic semigroups, and G, of all finite groups, are pseudovarieties of semigroups.

On the language side, the properties of a language may depend on the alphabet on which it is considered. To take into account the alphabet, one defines a *variety of rational languages* to be a correspondence $\mathcal{V}$ associating to each finite alphabet A a Boolean subalgebra $\mathcal{V}(A^+)$ of $\mathcal{P}(A^+)$ such that

(1) if $L \in \mathcal{V}(A^+)$ and $a \in A$ then the *quotient* languages $a^{-1}L = \{w : aw \in L\}$ and $La^{-1} = \{w : wa \in L\}$ belong to $\mathcal{V}(A^+)$ (*closure under quotients*);

(2) if $\varphi : A^+ \to B^+$ is a homomorphism and $L \in \mathcal{V}(B^+)$ then the inverse image $\varphi^{-1}L$ belongs to $\mathcal{V}(A^+)$ (*closure under inverse homomorphic images*).

For example, the correspondence which associates with each finite alphabet the set of all plus-free languages over it is a variety of rational languages. The correspondence between varieties of rational languages and pseudovarieties is easily described in terms of the syntactic semigroup as follows:

- associate with each variety of rational languages $\mathcal{V}$ the pseudovariety V generated by all syntactic semigroups $\operatorname{Synt} L$ with $L \in \mathcal{V}(A^+)$;

- associate with each pseudovariety V of finite semigroups the correspondence

$$\begin{aligned}\mathcal{V} : A \mapsto \mathcal{V}(A^+) &= \{L \subseteq A^+ : \operatorname{Synt} L \in \mathsf{V}\} \\ &= \{L \subseteq A^+ : L \text{ is recognized by some } S \in \mathsf{V}\}\end{aligned}$$

Since intersections of non-empty families of pseudovarieties are again pseudovarieties, pseudovarieties of semigroups constitute a complete lattice for the inclusion ordering. Similarly, one may order varieties of languages by putting $\mathcal{V} \leq \mathcal{W}$ if $\mathcal{V}(A^+) \subseteq \mathcal{W}(A^+)$ for every finite alphabet A. Then every non-empty family of varieties $(\mathcal{V}_i)_{i\in I}$ admits the infimum $\mathcal{V}$ given by $\mathcal{V}(A^+) = \bigcap_{i\in I} \mathcal{V}_i(A^+)$ and so again the varieties of rational languages constitute a complete lattice.

2.6 Theorem (Eilenberg [36]) *The above two correspondences are mutually inverse isomorphisms between the lattice of varieties of rational languages and the lattice of pseudovarieties of finite semigroups.*

Schützenberger's Theorem provides an instance of this correspondence, but of course this by no means says that that theorem follows from Eilenberg's Theorem. See M. V. Volkov's lecture notes in this volume and Section 5 for another important "classical" instance of Eilenberg's correspondence, namely Simon's Theorem relating the variety of so-called piecewise testable languages with the pseudovariety J of finite semigroups in which every principal ideal admits a unique element as a generator. See Eilenberg [36] and Pin [65] for many more examples.

2.7 Example An elementary example which is easy to treat here is the correspondence between the variety $\mathcal{N}$ of finite and cofinite languages and the pseudovariety N of all finite nilpotent semigroups. We say that a semigroup S is *nilpotent* if there exists a positive integer n such that all products of n elements of S are equal; the least such n is called the *nilpotency index* of S. The common value of all sufficiently long products in a nilpotent semigroup must of course be zero. If the alphabet A is finite, the finite semigroup S is nilpotent with nilpotency index n, and the homomorphism $\varphi : A^+ \to S$ recognizes the language L, then either φL does not contain zero, so that L must consist of words of length smaller than n which implies L is finite, or φL contains zero and then every word of length at least n must lie in L, so that the complement of L is finite.

Since N is indeed a pseudovariety and the correspondence $\mathcal{N}$ associating with a finite alphabet A the set of all finite and cofinite languages $L \subseteq A^+$ is a variety of rational languages, to prove the converse it suffices, by Eilenberg's Theorem, to show that every singleton language $\{w\}$ over a finite alphabet A is recognized by a finite nilpotent semigroup. Now, given a finite alphabet A and a positive integer n, the set I_n of all words of length greater than n is an ideal of the free semigroup A^+ and the Rees quotient A^+/I_n, in which all words of I_n are identified to a zero element, is a member of N. If $w \notin I_n$, that is if the length $|w|$ of w satisfies $|w| \leq n$, then the quotient homomorphism $A^+ \to A^+/I_n$ recognizes $\{w\}$. Hence we have $\mathsf{N} \leftrightarrow \mathcal{N}$ via Eilenberg's correspondence.

Eilenberg's correspondence gave rise to a lot of research aimed at identifying pseudovarieties of finite semigroups corresponding to combinatorially defined varieties of rational languages and, conversely, varieties of rational languages corresponding to algebraically defined pseudovarieties of finite semigroups.

Another aspect of the research is explained in part by the different character of the two directions of Eilenberg's correspondence. The pseudovariety V associated with a variety $\mathcal{V}$ of rational languages is defined in terms of generators. Nevertheless, Proposition 2.5 shows how to recover from a given semigroup $S \in \mathsf{V}$ an expression for S as a divisor of a product of generators so that a finite semigroup S belongs to V if and only if the languages computed from S according to Proposition 2.5 belong to $\mathcal{V}$.

On the other hand, if we could effectively test membership in V, then we could effectively determine if a rational language $L \subseteq A^+$ belongs to $\mathcal{V}(A^+)$: we would simply compute the syntactic semigroup of L and test whether it belongs to V, the answer being also the answer to the question of whether $L \in \mathcal{V}(A^+)$. This raises the most common problem encountered in finite semigroup theory: given a pseudovariety V defined in terms of generators, determine whether it has a decidable membership problem. A pseudovariety with this property is said to be *decidable*. Since for instance for each set P of primes, the pseudovariety consisting of all finite groups G such that the prime factors of $|G|$ belong to P determines P, a simple counting argument shows that there are too many pseudovarieties for all of them to be decidable. For natural constructions of undecidable pseudovarieties from decidable ones see [1, 24].

For the reverse direction, given a pseudovariety V one is often interested in natural and combinatorially simple generators for the associated variety $\mathcal{V}$ of rational languages. These generators are often defined in terms of Boolean operations: for each finite alphabet A a "natural" generating subset for the Boolean algebra $\mathcal{V}(A^+)$ should be identified. For instance, a language $L \subseteq A^+$ is *piecewise testable* if and only if it is a Boolean combination of languages of the form $A^*a_1A^* \cdots a_nA^*$ with $a_1, \ldots, a_n \in A$. We will run again into this kind of question in Subsection 3.3 where it will be given a simple topological formulation.

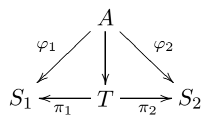
3 Free objects

A basic difficulty in dealing with pseudovarieties of finite algebraic structures is that in general they do not have free objects. The reason is quite simple: free objects tend to be infinite.

As a simple example, consider the pseudovariety N of all finite nilpotent semigroups. For a finite alphabet A and a positive integer n, denoting again by I_n the set of all words of length greater than n, the Rees quotient A^+/I_n belongs to N. In particular, there are arbitrarily large A-generated finite nilpotent semigroups and therefore there can be none which is free among them. In general, there is an A-generated free member of a pseudovariety V if and only if up to isomorphism there are only finitely many A-generated members of V, and most interesting pseudovarieties of semigroups fail this condition.

In universal algebraic terms, we could consider the free objects in the variety generated by V. This variety is defined by all identities which are valid in V and for instance for N there are no such nontrivial semigroup identities: in the notation of the preceding paragraph, A^+/I_n satisfies no nontrivial identities in at most $|A|$ variables in which both sides have length at most n. This means that if we take free objects in the algebraic sense then we lose a lot of information since in particular all pseudovarieties containing N will have the same associated free objects.

Let us go back and try to understand better what is meant by a free object. The idea is to take a structure which is just as general as it needs to be in order to be more general than all A-generated members of a given pseudovariety V. Let us take two A-generated members of V, say given by functions $\varphi_i : A \to S_i$ such that $\varphi_i(A)$ generates S_i $(i = 1, 2)$. Let T be the subsemigroup of the product generated by all pairs of the form $(\varphi_1(a), \varphi_2(a))$ with $a \in A$. Then T is again an A-generated member of V and we have the commutative diagram



where $\pi_i : T \to S_i$ is the projection on the ith component. The semigroup T is therefore more general than both S_1 and S_2 as an A-generated member of V and it is as small as possible to satisfy this property. We could keep going on doing this with more and more A-generated members of V but the problem is that we know, by the above discussion concerning N, that in general we will never end up with one member of V which is more general than all the others. So we need some kind of limiting process. The appropriate construction is the projective (or inverse) limit which we proceed to introduce in the somewhat wider setting of topological semigroups.

3.1 Profinite semigroups

By a *directed set* we mean a poset in which any two elements have a common upper bound. A subset C of a poset P is said to be *cofinal* if, for every element $p \in P$, there exists $c \in C$ such $p \leq c$.

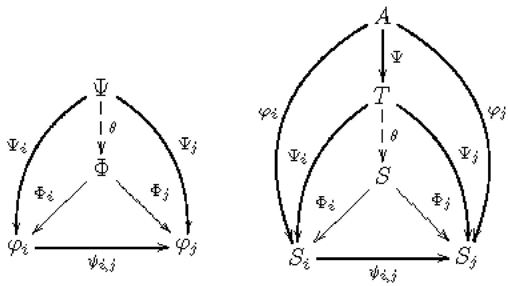
By a *topological semigroup* we mean a semigroup S endowed with a topology such that the semigroup operation $S \times S \to S$ is continuous. Fix a set A and consider the category of *A-generated topological semigroups* whose objects are the mappings $A \to S$ into topological semigroups whose images generate dense subsemigroups, and whose morphisms $\theta : \varphi \to \psi$, from $\varphi : A \to S$ to $\psi : A \to T$, are given by continuous homomorphisms $\theta : S \to T$ such that $\theta \circ \varphi = \psi$. Now, consider a *projective system* in this category, given by a directed set I of indices, for each $i \in I$ an object $\varphi_i : A \to S_i$ in our category of A-generated topological semigroups and, for each pair $i, j \in I$ with $i \geq j$, a *connecting* morphism $\psi_{i,j} : \varphi_i \to \varphi_j$ such that the following conditions hold for all $i, j, k \in I$:

- $\psi_{i,i}$ is the identity morphism on φ_i;
- if $i \geq j \geq k$ then $\psi_{j,k} \circ \psi_{i,j} = \psi_{i,k}$.

The *projective limit* of this projective system is an A-generated topological semigroup $\Phi : A \to S$ together with morphisms $\Phi_i : \Phi \to \varphi_i$ such that for all $i, j \in I$ with $i \geq j$, $\psi_{i,j} \circ \Phi_i = \Phi_j$ and, moreover, the following universal property holds:

> *For any other A-generated topological semigroup $\Psi : A \to T$ and morphisms $\Psi_i : \Psi \to \varphi_i$ such that for all $i, j \in I$ with $i \geq j$, $\psi_{i,j} \circ \Psi_i = \Psi_j$ there exists a morphism $\theta : \Psi \to \Phi$ such that $\Phi_i \circ \theta = \Psi_i$ for every $i \in I$.*

The situation is depicted in the following two commutative diagrams of morphisms and mappings respectively:



The uniqueness up to isomorphism of such a projective limit is a standard diagram chasing exercise. Existence may be established as follows.

Consider the subsemigroup S of the product $\prod_{i\in I} S_i$ consisting of all $(s_i)_{i\in I}$ such that, for all $i, j \in I$ with $i \geq j$,

$$\varphi_{i,j}(s_i) = s_j \tag{3.1}$$

endowed with the induced topology from the product topology. To check that S provides a construction of the projective limit, we first claim that the mapping $\Phi : A \to S$ given by $\Phi(a) = (\varphi_i(a))_{i\in I}$ is such that $\Phi(A)$ generates a dense subsemigroup T of S. Indeed, since the system is projective, to find an approximation $(t_i)_{i\in I} \in T$ to an element $(s_i)_{i\in I}$ of S given by $t_{i_j} \in K_{i_j}$ for a clopen set $K_{i_j} \subseteq S_{i_j}$ containing s_{i_j} with $j = 1, \ldots, n$, one may first take $k \in I$ such that $k \geq i_1, \ldots, i_n$. Then, by the hypothesis that the subsemigroup T_k of S_k generated by $\varphi_k(A)$ is dense, there is a word $w \in A^+$ which in T_k represents an element of the open set $\bigcap_{j=1}^{n} \psi_{k,i_j}^{-1} K_{i_j}$ since this set is non-empty as s_k belongs to it. This word w then represents an element $(t_i)_{i\in I}$ of T which is an approximation as required.

It is now an easy exercise to show that the projections $\Phi_i : S \to S_i$ have the above universal property. Note that since each of the conditions (3.1) only involves two components and $\varphi_{i,j}$ is continuous, S is a closed subsemigroup of the product $\prod_{i\in I} S_i$. So, by Tychonoff's Theorem, if all the S_i are compact semigroups, then so is S. We assume Hausdorff's separation axiom as part of the definition of compactness.

Recall that a topological space is *totally disconnected* if its connected components are singletons and it is *zero-dimensional* if it admits a basis of open sets consisting of clopen (meaning both closed and open) sets. See Willard [93] for a background in General Topology.

A finite semigroup is always viewed in this paper as a topological semigroup under the discrete topology. A *profinite semigroup* is defined to be a projective limit of a projective system of finite semigroups in the above sense, that is for some suitable choice of generators. The next result provides several alternative definitions of profinite semigroups.

3.1 Theorem *The following conditions are equivalent for a compact semigroup S:*

(1) *S is profinite;*

(2) *S is residually finite as a topological semigroup;*

(3) *S is a closed subdirect product of finite semigroups;*

(4) *S is totally disconnected;*

(5) *S is zero-dimensional.*

Proof By the explicit construction of the projective limit we have (1) $\Rightarrow$ (2) while (2) $\Rightarrow$ (3) is easily verified from the definitions. For (3) $\Rightarrow$ (1), suppose that $\Phi : S \to \prod_{i\in I} S_i$ is an injective continuous homomorphism from the compact semigroup S into a product of finite semigroups and that the factors are such that, for each component projection $\pi_j : \prod_{i\in I} S_i \to S_j$ the mapping $\pi_j \circ \Phi : S \to S_j$ is onto. We build a projective system of S-generated finite semigroups by considering all onto mappings of the form $\Phi_F : S \to S_F$ where F is a finite subset of I and $\Phi_F = \pi_F \circ \Phi$ where $\pi_F : \prod_{i\in I} S_i \to \prod_{i\in F} S_i$ denotes the natural projection; the indexing set is therefore the directed set of all finite subsets of I, under the inclusion ordering, and for the connecting homomorphisms we take the natural projections. It is now immediate to verify that S is the projective limit of this projective system of finite S-generated semigroups.

Since a product of totally disconnected spaces is again totally disconnected, we have (3) $\Rightarrow$ (4). The equivalence (4) $\Leftrightarrow$ (5) holds for any compact space and it is a well-known exercise in General Topology [93].

Up to this point in the proof, the fact that we are dealing with semigroups rather than any other variety of universal algebras really makes no essential difference. To complete the proof we establish the implication (5) $\Rightarrow$ (2), which was first proved by Numakura [62]. Given two distinct points $s, t \in S$, by zero-dimensionality they may be separated by a clopen subset $K \subseteq S$ in the sense that s lies in K and t does not. Since the syntactic congruence ρ_K saturates K, the congruence classes of s and t are distinct, that is the quotient homomorphism $\varphi : S \to \operatorname{Synt} K$ sends s and t to two distinct points. Hence, to prove (2) it suffices to show that $\operatorname{Synt} K$ is finite and φ is continuous, which is the object of Lemma 3.3 below. □

As an immediate application we obtain the following closure properties for the class of profinite semigroups.

3.2 Corollary *A closed subsemigroup of a profinite semigroup is also profinite. The product of profinite semigroups is also profinite.*

The following technical result has been extended in [2] to a universal algebraic setting in which syntactic congruences are determined by finitely many terms. See [32] for the precise scope of validity of the implication (5) $\Rightarrow$ (1) in Theorem 3.1 and applications in Universal Algebra.

We say that a congruence ρ on a topological semigroup is *clopen* if its classes are clopen.

3.3 Lemma (Hunter [44]) *If S is a compact zero-dimensional semigroup and K is a clopen subset of S then the syntactic congruence ρ_K is clopen, and therefore it has finitely many classes.*

Proof The proof uses nets, sequences indexed by directed sets which play for general topological spaces the role played by usual sequences for metric spaces [93]. Let $(s_i)_{i\in I}$ be a convergent net in S with limit s. We should show that there exists $i_0 \in I$ such that, whenever $i \geq i_0$, we have $s_i \mathrel{\rho_K} s$. Suppose on the contrary that for every $j \in I$ there exists $i \geq j$ such that s_i is not in the same ρ_K-class as s. The set Λ consisting of all $i \in I$ such that