

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison, UK

Josef Kittler, UK

Alfred Kobsa, USA

John C. Mitchell, USA

Oscar Nierstrasz, Switzerland

Bernhard Steffen, Germany

Demetri Terzopoulos, USA

Gerhard Weikum, Germany

Takeo Kanade, USA

Jon M. Kleinberg, USA

Friedemann Mattern, Switzerland

Moni Naor, Israel

C. Pandu Rangan, India

Doug Tygar, USA

Advanced Research in Computing and Software Science

Subline of Lectures Notes in Computer Science

Subline Series Editors

Giorgio Ausiello, *University of Rome 'La Sapienza', Italy*

Vladimiro Sassone, *University of Southampton, UK*

Subline Advisory Board

Susanne Albers, *University of Freiburg, Germany*

Benjamin C. Pierce, *University of Pennsylvania, USA*

Bernhard Steffen, *University of Dortmund, Germany*

Deng Xiaotie, *City University of Hong Kong*

Jeannette M. Wing, *Microsoft Research, Redmond, WA, USA*

Alberto Pardo Alfredo Viola (Eds.)

LATIN 2014: Theoretical Informatics

11th Latin American Symposium
Montevideo, Uruguay, March 31 – April 4, 2014
Proceedings



Springer

Volume Editors

Alberto Pardo
Universidad de la República
Facultad de Ingeniería
Instituto de Computación
Julio Herrera y Reissig 565
11300 Montevideo, Uruguay
E-mail: pardo@fing.edu.uy

Alfredo Viola
Universidad de la República
Facultad de Ingeniería
Instituto de Computación
Julio Herrera y Reissig 565
11300 Montevideo, Uruguay
E-mail: viola@fing.edu.uy

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-54422-4

e-ISBN 978-3-642-54423-1

DOI 10.1007/978-3-642-54423-1

Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014931658

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2014

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at the 11th Latin American Theoretical INformatics Symposium (LATIN 2014) held during March 31-April 4, 2014 in Montevideo, Uruguay. Previous editions of LATIN took place in São Paulo, Brazil (1992), Valparaíso, Chile (1995), Campinas, Brazil (1998), Punta del Este, Uruguay (2000), Cancún, México (2002), Buenos Aires, Argentina (2004), Valdivia, Chile (2006), Buzios, Brazil (2008), Oaxaca, México (2010) and Arequipa, Perú (2012).

The conference received 192 submissions from 42 countries. Each submission was reviewed by at least three Program Committee members, and carefully evaluated on quality, originality, and relevance to the conference. Overall, the Committee members wrote 588 reviews with the help of 254 external referees. Based on an extensive electronic discussion, the Committee selected 65 papers, leading to an acceptance rate of 34%. In addition to the accepted contributions, the symposium featured distinguished lectures by Ronitt Rubinfeld (Massachusetts Institute of Technology and Tel Aviv University), Robert Sedgewick (Princeton University), Gilles Barthe (IMDEA Software Institute), Gonzalo Navarro (Universidad de Chile), and J. Ian Munro (University of Waterloo).

The Imre Simon Test-of-Time Award started in 2012 and it is given to the authors of the LATIN paper deemed to be most influential among all those published at least ten years prior to the current edition of the conference. Papers published in the LATIN proceedings up to and including 2004 were eligible for the 2014 award. This year's winners were Graham Cormode and Sethu Muthu Muthukrishnan for their paper "An improved data stream summary: The count-min sketch and its applications", which appeared in LATIN 2004.

Many people helped to make LATIN 2014 possible. First, I would like to recognize the outstanding work of the members of the Program Committee. Their commitment contributed to a very detailed discussion on each of the submitted papers. The LATIN Steering Committee offered valuable advice and feedback; the conference benefitted immensely from their knowledge and experience. I would also like to recognize J. Ian Munro, Yoshiharu Kohayakawa and Michael Bender for their work in the Imre Simon Test-of-Time Award Committee.

Our industrial sponsors, Yahoo! Labs and Google provided much-needed funding. In particular, Yahoo! provided funds for the Imre Simon Award and Google for student grants. I thank Ricardo Baeza-Yates, Ravi Kumar and Prabhakar Raghavan for serving as contacts to those institutions.

The Centro Latinoamericano de Estudios en Informática (CLEI), the Comisión Sectorial de Investigaciones Científicas de la Universidad de la República (CSIC), the Programa de Desarrollo de las Ciencias Básicas (PEDECIBA) and the Agencia Nacional de Investigación e Innovación (ANII) also provided important seed

funding. The Universidad ORT supported all the graphic design for the conference.

At the Universidad de la República, Alberto Pardo chaired the Local Arrangements Committee. His outstanding commitment in the most difficult moments of the organization was key to the success of LATIN. Guillermo Calderón administered the conference web site. The rest of the Local Arrangements Committee, Javier Molina, Laura Molina and Alfonsina Pastori ably handled the innumerable logistical details that had to be resolved along the way. Finally, I thank my wife Graciela Pastori for the encouragement she offered during the year and a half that it took to make LATIN 2014 a reality.

January 2014

Alfredo Viola

Organization

Program Committee

Ricardo Baeza-Yates	Yahoo! Labs, Spain
Jérémy Barbay	Universidad de Chile, Chile
Michael Bender	Stony Brook University, USA
Joan Boyar	University of Southern Denmark, Denmark
Vida Dujmovic	McGill University, Canada
Leah Epstein	University of Haifa, Israel
Cristina Fernandes	Universidade de São Paulo, Brazil
Maribel Fernandez	KCL London, England
Joachim von zur Gathen	University of Bonn, Germany
Gaston Gonnet	ETH Zurich, Switzerland
Marcos Kiwi	Universidad de Chile, Chile
Yoshiharu Kohayakawa	University of São Paulo, Brazil
Evangelos Kranakis	Carleton University, Canada
Ravi Kumar	Google, USA
Anna Lubiw	University of Waterloo, Canada
Conrado Martínez	Universitat Politècnica de Catalunya, Spain
Elvira Mayordomo	Universidad de Zaragoza, Spain
Marco Molinaro	Carnegie Mellon University, USA
Regina Motz	Universidad de la República, Uruguay
Lucia Moura	University of Ottawa, Canada
Daniel Panario	Carleton University, Canada
Sergio Rajsbaum	Universidad Nacional Autónoma de México, Mexico
Tamara Rezk	Inria, France
Andrea Richa	Arizona State University, USA
Jacques Sakarovitch	CNRS / ENST Paris, France
Nicolas Schabanel	CNRS - Université Paris Diderot (Paris 7), France
Rodrigo Silveira	Universitat Politècnica de Catalunya, Spain
Jose A. Soto	Universidad de Chile, Chile
Martin Strauss	University of Michigan, USA
Vilmar Trevisan	UFRGS, Brazil
Jorge Urrutia	Universidad Nacional Autónoma de México, Mexico
Tarmo Uustalu	Tallinn University of Technology, Estonia
Brigitte Vallée	CNRS/University of Caen, France
Alfredo Viola (Chair)	Universidad de la República, Uruguay
Santiago Zanella-Béguelin	Microsoft Research, England

Local Arrangements Committee

Guillermo Calderón
Javier Molina
Laura Molina

Alfonsina Pastori
Alberto Pardo (chair)

Steering Committee

David Fernández-Baca
Eduardo Sany Laber
Alejandro López-Ortiz
Gonzalo Navarro
Marie-France Sagot

Iowa State University, USA
PUC- Rio, Brazil
University of Waterloo, Canada
Universidad de Chile, Chile
Inria Grenoble Rhône-Alpes and Université
Claude Bernard (Lyon 1), France
Universidade de São Paulo, Brazil

Imre Simon Test-of-Time Award Committee

Michael Bender
Yoshiharu Kohayakawa
J. Ian Munro (Chair)

Stony Brook University, USA
Universidade de São Paulo, Brazil
University of Waterloo, Canada

Sponsors

ANII (Agencia Nacional de Investigación e Innovación), Uruguay
CLEI (Centro Latinoamericano de Estudios en Informática)
CSIC (Comisión Sectorial de Investigación Científica, Universidad
de la República), Uruguay
Google, USA
PEDECIBA Informática (Programa de Desarrollo de las Ciencias Básicas), Uruguay
Universidad ORT, Uruguay
Yahoo! Labs, Spain

Additional Reviewers

Abdessalem, Talel
Addario-Berry, Louigi
Afshani, Peyman
Akhavi, Ali
Angelini, Patrizio
Antoniadis, Antonios
Ayala-Rincon, Mauricio
Aziz, Haris

Bacher, Axel
Bampas, Evangelos
Barba, Luis
Barcelo, Pablo
Bauer, Andrej
Bazgan, Cristina
Bernardi, Olivier
Bodini, Olivier

Bonomo, Flavia
 Bose, Prosenjit
 Brandstadt, Andreas
 Brewster, Rick
 Brizuela, Carlos
 Buchbinder, Niv
 Buchin, Maike
 Bulteau, Laurent
 Buratti, Marco
 Buriol, Luciana
 Cai, Leizhen
 Calinescu, Gruia
 Camarão, Carlos
 Campos, Victor
 Castaneda, Armando
 Castelli Aleardi, Luca
 Chalermsook, Parinya
 Chalopin, Jérémie
 Chapelle, Mathieu
 Chen, Yuxin
 Chierichetti, Flavio
 Christodoulakis, Manolis
 Clément, Julien
 Corteel, Sylvie
 Costello, Kevin
 Couillec, Yoann
 Courcelle, Bruno
 Csirmaz, Laszlo
 Damian, Mirela
 Dantas, Simone
 Daudé, Hervé
 David, Julien
 de Carli Silva, Marcel
 De La Clergerie, Eric
 de Pina, José Coelho
 de Rezende, Pedro J.
 de Vries, Fer-Jan
 Delgado, Jordi
 Delporte-Gallet, Carole
 Devismes, Stéphane
 Dobrev, Stefan
 Doerr, Benjamin
 Dourado, Mitre
 Drmota, Michael
 Duchon, Philippe
 Duffy, Chris
 Duncan, Christian
 Elizalde, Sergi
 Eppstein, David
 Esfandiari, Hossein
 Fabrikant, Alex
 Fagerberg, Rolf
 Faliszewski, Piotr
 Fauconnier, Hugues
 Favrholt, Lene Monrad
 Feige, Uriel
 Fertin, Guillaume
 Fiala, Jiri
 Find, Magnus
 Flocchini, Paola
 Fomin, Fedor
 Fonseca, Guilherme
 Fournier, Hervé
 Fragoso Santos, Jose
 Frati, Fabrizio
 Ganapathi, Pramod
 Gao, Jie
 Gao, Shuhong
 Gao, Zhicheng
 Garg, Vijay
 Gargano, Luisa
 Gaspers, Serge
 Georgiou, Konstantinos
 Geremia, Ezequiel
 Gittenberger, Bernhard
 Green, Oded
 Grossi, Roberto
 Guha, Sudipto
 Gutin, Gregory
 Harutyunyan, Anna
 Havet, Frederic
 He, Meng
 Hernandez, Cecilia
 Hoppen, Carlos
 Horak, Peter
 Huang, Chien-Chung
 Hwang, Hsien-Kuei
 Hüffner, Falk
 Ilcinkas, David
 Iljazović, Zvonko

Im, Sungjin
 Jansen, Bart
 Jansen, Klaus
 Jež, Artur
 Jimenez, Andrea
 Josuat-Verges, Matthieu
 Jungnickel, Dieter
 Kanagal, Bhargav
 Kiazyk, Stephen
 King, James
 Klostermeyer, Chip
 Kniesburgess, Sebastian
 Kobourov, Stephen
 Kononov, Alexander
 Korman, Matias
 Kosowski, Adrian
 Kratochvil, Jan
 Krivelevich, Michael
 Krumke, Sven
 Kuhn, Daniela
 Kuznetsov, Petr
 Labarre, Anthony
 Lamb, Luis
 Langerman, Stefan
 Larsen, Kim S.
 Lattanzi, Silvio
 Lecroq, Thierry
 Lee, Sang June
 Lefmann, Hanno
 Leme, Renato
 Levin, Asaf
 Lhote, Loick
 Li, Minming
 Loebenberger, Daniel
 Lozano, Antoni
 Lozin, Vadim
 Lugosi, Gabor
 Lumbroso, Jérémie
 Löffler, Maarten
 MacQuarrie, Fraser
 Mahdian, Mohammad
 Makowsky, Johann
 Mandel, Arnaldo
 Mansour, Toufik
 Margalit, Oded
 Markou, Euripides
 Martin, Russell
 Martinez-Moro, Edgar
 Martins, Enide
 Martín, Álvaro
 McCauley, Samuel
 Meer, Klaus
 Milani, Alessia
 Milanič, Martin
 Molinero, Xavier
 Morales Ponce, Oscar
 Moseley, Benjamin
 Mota, Guilherme O.
 Moura, Arnaldo
 Mucha, Marcin
 Mueller, Moritz
 Musicante, Martin
 Nagarajan, Viswanath
 Nantes, Daniele
 Navarro, Gonzalo
 Neschachnow, Sergio
 Nilsson, Bengt
 Nüsken, Michael
 Ollinger, Nicolas
 Ott, Sebastian
 Pacheco, Eduardo
 Pagourtzis, Aris
 Pajak, Dominik
 Panagiotou, Konstantinos
 Pathak, Vinayak
 Paulusma, Daniel
 Perez, Anthony
 Perret, Ludovic
 Pighizzini, Giovanni
 Pilz, Alexander
 Ponty, Yann
 Popa, Alex
 Pott, Alexander
 Pruhs, Kirk
 Pérez-Lantero, Pablo
 Rad, Nader Jafari
 Radke, Klaus
 Raekow, Yona
 Rahman, M. Sohail
 Reyes, Nora

Richmond, Bruce
Rojas, Javiel
Saket, Rishi
Salinger, Alejandro
Salvy, Bruno
Sam, Sethserey
Sampaio, Rudini
Sato, Cristiane M.
Saumell, Maria
Saurabh, Saket
Sawada, Joe
Schaudt, Oliver
Schmid, Stefan
Schouery, Rafael
Schwartz, Roy
Seara, Carlos
Sereni, Jean-Sébastien
Serpette, Bernard
Shah, Rahul
Shirazipourazad, Shahrzad
Singer, Yaron
Sitchinava, Nodari
Soria, Michele
Sotelo, David
Stein, Maya
Stewart, Lorna
Stiller, Sebastian
Sviridenko, Maxim
Swenson, Krister

Tamir, Arie
Tannier, Eric
Telha, Claudio
Thraves, Christopher
Toft, Bjarne
Tomkins, Andrew
Tran, Huong
Travers, Corentin
Tsichlas, Kostas
Uchizawa, Kei
Umboh, Seeun
V. Silva, Pedro
van Leeuwen, Erik Jan
van Stee, Rob
Vassilvitskii, Sergei
Vee, Erik
Venkatasubramanian, Suresh
Verdonschot, Sander
Viera, Marcos
Vigneron, Antoine
Villard, Gilles
Wakabayashi, Yoshiko
Weber, Ken
Xia, Donglin
Yamamura, Akihiro
Yen, Hsu-Chun
Ziegler, Konstantin
Ziegler, Martin
Zito, Michele

Abstracts

Something for Almost Nothing: Advances in Sub-linear Time Algorithms

Ronitt Rubinfeld

CSAIL, MIT, Cambridge MA 02139

Blavatnik School of Computer Science, Tel Aviv University

`ronitt@csail.mit.edu`

Abstract. Linear-time algorithms have long been considered the gold standard of computational efficiency. Indeed, it is hard to imagine doing better than that, since for a nontrivial problem, any algorithm must consider all of the input in order to make a decision. However, as extremely large data sets are pervasive, it is natural to wonder what one can do in sub-linear time. Over the past two decades, several surprising advances have been made on designing such algorithms. We will give a non-exhaustive survey of this emerging area, highlighting recent progress and directions for further research.

Computer-Aided Cryptographic Proofs

Gilles Barthe

IMDEA Software Institute
`gilles.barthe@imdea.org`

`EasyCrypt` [6] is a computer-assisted framework for reasoning about the security of cryptographic constructions, using the methods and tools of provable security, and more specifically of the game-based techniques. The core of `EasyCrypt` is a relational program logic for a core probabilistic programming language with sequential composition, conditionals, loops, procedure calls, assignments and sampling from discrete distributions. The relational program logic is key to capture reductionist arguments that arise in cryptographic proofs. It is complemented by a (standard, non-relational) program logic that allows to reason about the probability of events in the execution of probabilistic programs; this program logic allows for instance to upper bound the probability of failure events, that are pervasive in game-based cryptographic proofs. In combination, these logics capture general reasoning principles in cryptography and have been used to verify the security of emblematic constructions, including the Full-Domain Hash signature [8], the Optimal Asymmetric Encryption Padding (OAEP) [7], hash function designs [3] and zero-knowledge protocols [5, 1]. Yet, these logics can only capture instances of general principles, and lack mechanisms for stating and proving these general principles once and for all, and then for instantiating them as needed. To overcome this limitation, we have recently extended `EasyCrypt` with programming language mechanisms such as modules and type classes. Modules provide support for composition of cryptographic proofs, and for formalizing hybrid arguments, whereas type classes are convenient to model and reason about algebraic structures. Together, these extensions significantly expand the class of examples that can be addressed with `EasyCrypt`. For instance, we have used the latest version of `EasyCrypt` to verify the security of a class of authenticated key exchange protocols, and of a secure function evaluation protocol based on garbled circuits and oblivious transfer.

Our current work explores two complementary directions. On the one hand, we are extending the `EasyCrypt` infrastructure in order to derive security guarantees about implementations of cryptographic constructions. Indeed, practical attacks often target specific implementations and exploit some characteristics that are not considered in typical provable security proofs; as a consequence, several widely used implementations of provably secure schemes are vulnerable to attacks. In order to narrow the gap between provable security and implementations, we are extending `EasyCrypt` with support to reason about C-like implementations, and use the `CompCert` verified C compiler (<http://compcert.inria.fr/>) to carry the security guarantees down to executable implementations [2]. On the other hand, we are developing specialized formalisms to reason

about the security of particular classes of constructions. For instance, we have recently developed the **ZooCrypt** framework [4], which supports automated analysis of chosen-plaintext and chosen ciphertext-security for public-key encryption schemes built from (partial-domain) one-way trapdoor permutations and random oracles. Using **ZooCrypt**, we have analyzed over a million (automatically generated) schemes, including many schemes from the literature. For chosen-plaintext security, **ZooCrypt** is able to report in nearly 99% of the cases a proof of security with a concrete security bound, or an attack. We are currently extending our approach to reason about encryption schemes based on Diffie-Hellmann groups and bilinear pairings, both in the random oracle and in the standard models.

More information about the project is available from the project web page

<http://www.easycrypt.info>

References

1. Almeida, J.B., Barbosa, M., Bangerter, E., Barthe, G., Krenn, S., Zanella-Béguelin, S.: Full proof cryptography: verifiable compilation of efficient zero-knowledge protocols. In: 19th ACM Conference on Computer and Communications Security. ACM (2012)
2. Almeida, J.B., Barbosa, M., Barthe, G., Dupressoir, F.: Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations. In: ACM Conference on Computer and Communications Security. ACM (2013)
3. Backes, M., Barthe, G., Berg, M., Grégoire, B., Skoruppa, M., Zanella-Béguelin, S.: Verified security of Merkle-Damgård. In: IEEE Computer Security Foundations. ACM (2012)
4. Barthe, G., Crespo, J.M., Grégoire, B., Kunz, C., Lakhnech, Y., Schmidt, B., Zanella-Béguelin, S.: Automated analysis and synthesis of padding-based encryption schemes. In: ACM Conference on Computer and Communications Security. ACM (2013)
5. Barthe, G., Grégoire, B., Hedin, D., Heraud, S., Zanella-Béguelin, S.: A Machine-Checked Formalization of Sigma-Protocols. In: IEEE Computer Security Foundations. ACM (2010)
6. Barthe, G., Grégoire, B., Heraud, S., Zanella-Béguelin, S.: Computer-aided security proofs for the working cryptographer. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 71–90. Springer, Heidelberg (2011)
7. Barthe, G., Grégoire, B., Lakhnech, Y., Zanella-Béguelin, S.: Beyond Provable Security Verifiable IND-CCA Security of OAEP. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 180–196. Springer, Heidelberg (2011)
8. Zanella-Béguelin, S., Barthe, G., Grégoire, B., Olmedo, F.: Formally certifying the security of digital signature schemes. In: IEEE Symposium on Security and Privacy. IEEE Computer Society (2009)

“If You Can Specify It, You Can Analyze It” —The Lasting Legacy of Philippe Flajolet

Robert Sedgewick

Department of Computer Science, Princeton University
rs@cs.princeton.edu

Abstract. The “Flajolet School” of the analysis of algorithms and combinatorial structures is centered on an effective calculus, known as analytic combinatorics, for the development of mathematical models that are sufficiently accurate and precise that they can be validated through scientific experimentation. It is based on the generating function as the central object of study, first as a formal object that can translate a specification into mathematical equations, then as an analytic object whose properties as a function in the complex plane yield the desired quantitative results. Universal laws of sweeping generality can be proven within the framework, and easily applied. Standing on the shoulders of Cauchy, Polya, de Bruijn, Knuth, and many others, Philippe Flajolet and scores of collaborators developed this theory and demonstrated its effectiveness in a broad range of scientific applications. Flajolet’s legacy is a vibrant field of research that holds the key not just to understanding the properties of algorithms and data structures, but also to understanding the properties of discrete structures that arise as models in all fields of science. This talk will survey Flajolet’s story and its implications for future research.

“A man ... endowed with an an exuberance of imagination which puts it in his power to establish and populate a universe of his own creation”.

Encoding Data Structures

Gonzalo Navarro*

Department of Computer Science, University of Chile
gnavarro@dcc.uchile.cl

Classical data structures can be regarded as additional information that is stored on top of the raw data in order to speed up some kind of queries. Some examples are the suffix tree to support pattern matching in a text, the extra structures to support lowest common ancestor queries on a tree, or precomputed shortest path information on a graph.

Some data structures, however, can operate *without accessing the raw data*. These are called *encodings*. Encodings are relevant when they do not contain enough information to reproduce the raw data, but just what is necessary to answer the desired queries (otherwise, any data structure could be seen as an encoding, by storing a copy of the raw data inside the structure).

Encodings are interesting because they can occupy much less space than the raw data. In some cases the data itself is not interesting, only the answers to the queries on it, and thus we can simply discard the raw data and retain the encoding. In other cases, the data is used only sporadically and can be maintained in secondary storage, while the encoding is maintained in main memory, thus speeding up the most relevant queries.

When the raw data is available, any computable query on it can be answered with sufficient time. With encodings, instead, one faces a novel fundamental question: what is the *effective entropy* of the data with respect to a set of queries? That is, what is the minimum size of an encoding that can answer those queries without accessing the data? This question is related to Information Theory, but in a way inextricably associated to the data structure: the point is not how much information the data contains, but how much information is conveyed by the queries. In addition, as usual, there is the issue of how efficiently can be the queries answered depending on how much space is used.

In this talk I will survey some classical and new encodings, generally about preprocessing arrays $A[1, n]$ so as to answer queries on array intervals $[i, j]$ given at query time. I will start with the classical range minimum queries (which is the minimum value in $A[i, j]$?) which has a long history that culminated a few years ago in an asymptotically space-optimal encoding of $2n + o(n)$ bits answering queries in constant time. Then I will describe more recent (and partly open)

* Funded in part by Millennium Nucleus Information and Coordination in Networks ICM/FIC P10-024F, Chile.

problems such as finding the second minimum in $A[i, j]$, the k smallest values in $A[i, j]$, the k th smallest value in $A[i, j]$, the elements that appear more than a fraction τ of the times in $A[i, j]$, etc. All these queries appear recurrently within other algorithmic problems, and they have also direct application in data mining.

Succinct Data Structures ... Not Just for Graphs

J. Ian Munro

Cheriton School of Computer Science, University of Waterloo,
Waterloo, Ontario N2L 3G1, Canada
`imunro@uwaterloo.ca`

Abstract. Succinct data structures are data representations that use the (nearly) the information theoretic minimum space, for the combinatorial object they represent, while performing the necessary query operations in constant (or nearly constant) time. So, for example, we can represent a binary tree on n nodes in $2n + o(n)$ bits, rather than the "obvious" $5n$ or so *words*, i.e. $5n \lg n$ bits. Such a difference in memory requirements can easily translate to major differences in runtime as a consequence of the level of memory in which most of the data resides. The field developed to a large extent because of applications in text indexing, so there has been a major emphasis on trees and a secondary emphasis on graphs in general; but in this talk we will draw attention to a much broader collection of combinatorial structures for which succinct structures have been developed. These will include sets, permutations, functions, partial orders and groups, and yes, a bit on graphs.

Table of Contents

Complexity 1

Conjugacy in Baumslag’s Group, Generic Case Complexity, and Division in Power Circuits	1
<i>Volker Diekert, Alexei G. Myasnikov, and Armin Weiß</i>	
Hierarchical Complexity of 2-Clique-Colouring Weakly Chordal Graphs and Perfect Graphs Having Cliques of Size at Least 3	13
<i>Helio B. Macêdo Filho, Raphael C.S. Machado, and Celina M.H. Figueiredo</i>	
The Computational Complexity of the Game of Set and Its Theoretical Applications	24
<i>Michael Lampis and Valia Mitsou</i>	

Complexity 2

Independent and Hitting Sets of Rectangles Intersecting a Diagonal Line	35
<i>José R. Correa, Laurent Feuilloley, and José A. Soto</i>	
Approximating Vector Scheduling: Almost Matching Upper and Lower Bounds	47
<i>Nikhil Bansal, Tjark Vredeveld, and Ruben van der Zwaan</i>	
False-Name Manipulation in Weighted Voting Games Is Hard for Probabilistic Polynomial Time	60
<i>Anja Rey and Jörg Rothe</i>	
A Natural Generalization of Bounded Tree-Width and Bounded Clique-Width	72
<i>Martin Fürer</i>	

Computational Geometry 1

Optimal Algorithms for Constrained 1-Center Problems	84
<i>Luis Barba, Prosenjit Bose, and Stefan Langerman</i>	
A Randomized Incremental Approach for the Hausdorff Voronoi Diagram of Non-crossing Clusters	96
<i>Panagiotis Cheilaris, Elena Khramtcova, Stefan Langerman, and Evanthia Papadopoulou</i>	

Upper Bounds on the Spanning Ratio of Constrained Theta-Graphs	108
<i>Prosenjit Bose and André van Renssen</i>	

Computing the L_1 Geodesic Diameter and Center of a Simple Polygon in Linear Time	120
<i>Sang Won Bae, Matias Korman, Yoshio Okamoto, and Haitao Wang</i>	

Graph Drawing

The Planar Slope Number of Subcubic Graphs	132
<i>Emilio Di Giacomo, Giuseppe Liotta, and Fabrizio Montecchiani</i>	

Smooth Orthogonal Drawings of Planar Graphs	144
<i>Muhammad Jawaherul Alam, Michael A. Bekos, Michael Kaufmann, Philipp Kindermann, Stephen G. Kobourov, and Alexander Wolff</i>	

Drawing HV -Restricted Planar Graphs	156
<i>Stephane Durocher, Stefan Felsner, Saeed Mehrabi, and Debajyoti Mondal</i>	

Periodic Planar Straight-Frame Drawings with Polynomial Resolution	168
<i>Luca Castelli Aleardi, Éric Fusy, and Anatolii Kostrygin</i>	

Automata

A Characterization of Those Automata That Structurally Generate Finite Groups	180
<i>Ines Klimann and Matthieu Picantin</i>	

Linear Grammars with One-Sided Contexts and Their Automaton Representation	190
<i>Mikhail Barash and Alexander Okhotin</i>	

Computability

On the Computability of Relations on λ -Terms and Rice's Theorem - The Case of the Expansion Problem for Explicit Substitutions	202
<i>Edward Hermann Haeusler and Mauricio Ayala-Rincón</i>	

Computing in the Presence of Concurrent Solo Executions	214
<i>Maurice Herlihy, Sergio Rajsbbaum, Michel Raynal, and Julien Stainer</i>	

Algorithms on Graphs

Combining All Pairs Shortest Paths and All Pairs Bottleneck Paths Problems	226
<i>Tong-Wook Shinn and Tadao Takaoka</i>	
(Total) Vector Domination for Graphs with Bounded Branchwidth	238
<i>Toshimasa Ishii, Hirotaka Ono, and Yushi Uno</i>	
Computing the Degeneracy of Large Graphs	250
<i>Martín Farach-Colton and Meng-Tsung Tsai</i>	

Computational Geometry 2

Approximation Algorithms for the Geometric Firefighter and Budget Fence Problems	261
<i>Rolf Klein, Christos Levcopoulos, and Andrzej Lingas</i>	
An Improved Data Stream Algorithm for Clustering	273
<i>Sang-Sub Kim and Hee-Kap Ahn</i>	
Approximation Algorithms for the Gromov Hyperbolicity of Discrete Metric Spaces	285
<i>Ran Duan</i>	
A (7/2)-Approximation Algorithm for Guarding Orthogonal Art Galleries with Sliding Cameras	294
<i>Stephane Durocher, Omrit Filtser, Robert Fraser, Ali D. Mehrabi, and Saeed Mehrabi</i>	

Algorithms

Helly-Type Theorems in Property Testing	306
<i>Sourav Chakraborty, Rameshwar Pratap, Sasanka Roy, and Shubhangi Saraf</i>	
New Bounds for Online Packing LPs	318
<i>Matthias Englert, Nicolaos Matsakis, and Marcin Mucha</i>	
Improved Minmax Regret 1-Center Algorithms for Cactus Networks with c Cycles	330
<i>Binay Bhattacharya, Tsunehiko Kameda, and Zhao Song</i>	
Collision-Free Network Exploration	342
<i>Jurek Czyzowicz, Dariusz Dereniowski, Leszek Gąsieniec, Rafł Klasing, Adrian Kosowski, and Dominik Pająk</i>	

Random Structures

Powers of Hamilton Cycles in Pseudorandom Graphs	355
<i>Peter Allen, Julia Böttcher, Hiệp Hàn, Yoshiharu Kohayakawa, and Yury Person</i>	
Local Update Algorithms for Random Graphs	367
<i>Philippe Duchon and Romaric Duwigau</i>	
Odd Graphs Are Prism-Hamiltonian and Have a Long Cycle	379
<i>Felipe De Campos Mesquita, Letícia Rodrigues Bueno, and Rodrigo De Alencar Hausen</i>	
Relatively Bridge-Addable Classes of Graphs	391
<i>Colin McDiarmid and Kerstin Weller</i>	

Complexity on Graphs 1

$O(n)$ Time Algorithms for Dominating Induced Matching Problems	399
<i>Min Chih Lin, Michel J. Mizrahi, and Jayme L. Szwarcfiter</i>	
Coloring Graph Powers: Graph Product Bounds and Hardness of Approximation	409
<i>Parinya Chalermsook, Bundit Laekhanukit, and Danupon Nanongkai</i>	
Convexity in Partial Cubes: The Hull Number	421
<i>Marie Albenque and Kolja Knauer</i>	
Connected Greedy Colourings	433
<i>Fabrcio Benevides, Victor Campos, Mitre Dourado, Simon Griffiths, Robert Morris, Leonardo Sampaio, and Ana Silva</i>	

Analytic Combinatorics

On the Number of Prefix and Border Tables	442
<i>Julien Clément and Laura Giambruno</i>	
Probabilities of 2-Xor Functions	454
<i>Élie de Panafieu, Danièle Gardy, Bernhard Gittenberger, and Markus Kuba</i>	
Equivalence Classes of Random Boolean Trees and Application to the Catalan Satisfiability Problem	466
<i>Antoine Genitrini and Cécile Mailler</i>	

Analytic and Enumerative Combinatorics

The Flip Diameter of Rectangulations and Convex Subdivisions	478
<i>Eyal Ackerman, Michelle M. Allen, Gill Barequet, Maarten Löffler, Joshua Mermelstein, Diane L. Souvaine, and Csaba D. Tóth</i>	
Weighted Staircase Tableaux, Asymmetric Exclusion Process, and Eulerian Type Recurrences	490
<i>Pawel Hitczenko and Svante Janson</i>	
Counting and Generating Permutations Using Timed Languages	502
<i>Nicolas Basset</i>	

Complexity on Graphs 2

Semantic Word Cloud Representations: Hardness and Approximation Algorithms	514
<i>Lukas Barth, Sara Irina Fabrikant, Stephen G. Kobourov, Anna Lubiw, Martin Nöllenburg, Yoshio Okamoto, Sergey Pupyrev, Claudio Squarcella, Torsten Ueckerdt, and Alexander Wolff</i>	
The Complexity of Homomorphisms of Signed Graphs and Signed Constraint Satisfaction	526
<i>Florent Foucaud and Reza Naserasr</i>	
Complexity of Coloring Graphs without Paths and Cycles	538
<i>Pavol Hell and Shenwei Huang</i>	

Approximation Algorithms

Approximating Real-Time Scheduling on Identical Machines	550
<i>Nikhil Bansal, Cyriel Ruten, Suzanne van der Ster, Tjark Vredeveld, and Ruben van der Zwaan</i>	
Integrated Supply Chain Management via Randomized Rounding	562
<i>Lehilton L.C. Pedrosa and Maxim Sviridenko</i>	
The Online Connected Facility Location Problem	574
<i>Mário César San Felice, David P. Williamson, and Orlando Lee</i>	
Multiply Balanced k -Partitioning	586
<i>Amihood Amir, Jessica Fidler, Robert Krauthgamer, Liam Roditty, and Oren Sar Shalom</i>	
On Some Recent Approximation Algorithms for MAX SAT	598
<i>Matthias Poloczek, David P. Williamson, and Anke van Zuylen</i>	

Analysis of Algorithms

Packet Forwarding Algorithms in a Line Network	610
<i>Antonios Antoniadis, Neal Barcelo, Daniel Cole, Kyle Fox, Benjamin Moseley, Michael Nugent, and Kirk Pruhs</i>	
Survivability of Swarms of Bouncing Robots	622
<i>Jurek Czyzowicz, Stefan Dobrev, Evangelos Kranakis, and Eduardo Pacheco</i>	
Emergence of Wave Patterns on Kadanoff Sandpiles	634
<i>Kévin Perrot and Éric Rémila</i>	

Computational Algebra

A Divide and Conquer Method to Compute Binomial Ideals	648
<i>Deepanjan Kesh and Shashank K. Mehta</i>	
How Fast Can We Multiply Large Integers on an Actual Computer?	660
<i>Martin Fürer</i>	

Applications to Bioinformatics

Sorting Permutations by Prefix and Suffix Versions of Reversals and Transpositions	671
<i>Carla Negri Lintzmayer and Zanoni Dias</i>	
Algorithmic and Hardness Results for the Colorful Components Problems	683
<i>Anna Adamaszek and Alexandru Popa</i>	

Budget Problems

On the Stability of Generalized Second Price Auctions with Budgets	695
<i>Josep Díaz, Ioannis Giotis, Lefteris Kirousis, Evangelos Markakis, and Maria Serna</i>	
Approximation Algorithms for the Max-Buying Problem with Limited Supply	707
<i>Cristina G. Fernandes and Rafael C.S. Schouery</i>	
Budget Feasible Mechanisms for Experimental Design	719
<i>Thibaut Horel, Stratis Ioannidis, and S. Muthukrishnan</i>	

Algorithms and Data Structures

LZ77-Based Self-indexing with Faster Pattern Matching.....	731
<i>Travis Gagie, Paweł Gawrychowski, Juha Kärkkäinen, Yakov Nekrich, and Simon J. Puglisi</i>	
Quad- K -d Trees	743
<i>Nikolett Bereczky, Amalia Duch, Krisztián Németh, and Salvador Roura</i>	
Biased Predecessor Search.....	755
<i>Prosenjit Bose, Rolf Fagerberg, John Howat, and Pat Morin</i>	
Author Index	765