Lecture Notes in Computer Science 8392

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Advanced Research in Computing and Software Science

Subline of Lectures Notes in Computer Science

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

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 Arragements 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 Autonoma 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 Autonoma 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	Iowa State University, USA
Eduardo Sany Laber	PUC- Rio, Brazil
Alejandro López-Ortiz	University of Waterloo, Canada
Gonzalo Navarro	Universidad de Chile, Chile
Marie-France Sagot	Inria Grenoble Rhône-Alpes and Université Claude Bernard (Lyon 1), France
Yoshiko Wakabayashi	Universidade de São Paulo, Brazil

Imre Simon Test-of-Time Award Committee

Michael Bender	Stony Brook University, USA
Yoshiharu Kohayakawa	Universidade de São Paulo, Brazil
J. Ian Munro (Chair)	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
Favrholdt, 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
Jeż, Artur
Jimenez, Andrea
Josuat-Verges, Matthieu
Jungnickel, Dieter
Kanagal, Bhargav
Kiazyk, Stephen
King, James
Klostermeyer, Chip
Kniesburges, 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
Nesmachnow, 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. Sohel
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 endciency. 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 kth 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

Complexity 2

Computational Geometry 1

Graph Drawing

Automata

Computability

Algorithms on Graphs

Computational Geometry 2

Algorithms

Random Structures

Complexity on Graphs 1

Analytic Combinatorics

Analytic and Enumerative Combinatorics

Complexity on Graphs 2

Approximation Algorithms

Analysis of Algorithms

Computational Algebra

Aplications to Bioinformatics

Budget Problems

Algorithms and Data Structures