Lecture Notes in Computer Science 12542

More information about this subseries at http://www.springer.com/series/7407

Jean Claude Bajard · Alev Topuzoğlu (Eds.)

Arithmetic of Finite Fields

8th International Workshop, WAIFI 2020
Rennes, France, July 6–8, 2020
Revised Selected and Invited Papers

Springer

Editors
Jean Claude Bajard
Sorbonne Paris
Paris, France

Alev Topuzoğlu
Sabancı University
Istanbul, Turkey

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-68868-4 ISBN 978-3-030-68869-1 (eBook)
https://doi.org/10.1007/978-3-030-68869-1

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 8th International Workshop on the Arithmetic of Finite Fields (WAIFI 2020) was quite exceptional. It was originally planned to be held at the University of Rennes 1, France. However, like most meetings in 2020, it ended up as a virtual workshop, a shift due to the COVID-19 pandemic.

Without doubt, we all missed the face-to-face interaction that we value so much. On the other hand, the unusual format of the meeting made it accessible to a wider research community. Indeed, WAIFI 2020 attracted over 200 registered participants from all around the world.

The program consisted of five plenary and twelve contributed talks. The plenary speakers were André Chailloux (Inria, Paris, France), Elisa Gorla (University of Neuchâtel, Switzerland), Gary McGuire (University College Dublin, Ireland), Emmanuela Orsini (KU Leuven, Belgium) and Eric Schost (University of Waterloo, Canada). We invited the plenary speakers to contribute survey papers to the proceedings volume. We are very glad that Elisa Gorla, Gary McGuire and Emmanuela Orsini were able to allocate the time to prepare the manuscripts that are included in this volume. An extended abstract of the talk of André Chailloux is also included here. Video recordings of the talks of André Chailloux, Elisa Gorla, Emmanuela Orsini and Eric Schost can be found at http://waifi.org/program.html.

The number of submissions to WAIFI 2020 was rather low, which was not surprising, considering the uncertainties surrounding the COVID-19 pandemic. Out of the 22 fine papers, which received at least three single-blind reviews by PC members or external reviewers chosen by the members, 12 were selected after a discussion online. We are grateful to the Program Committee (PC) members and external reviewers for ensuring a rigorous reviewing process despite all the difficulties caused by the pandemic and the confinement measures. We are also grateful to the authors for agreeing to make video recordings presenting highlights of their papers, which are available on http://waifi.org/program.html.

We worked very closely and harmoniously with the general chairs Sylvain Duquesne and Arnaud Tisserand. Their engagement and hard work in leading the overall organization are much appreciated. Special thanks go to José Luis Imaña, the publicity chair, who also maintained the website with great care. Indeed, the website was viewed over 1600 times in the two weeks starting on 29 June 2020, when the programme was announced and the pre-recorded video presentations of selected papers were posted. We are also thankful to the Steering Committee for their continual support and acknowledge the brilliant work done by the Organizing Committee.

University of Rennes 1 provided the essential infrastructure. We are particularly thankful to INRIA, Lab-STICC CNRS and Centre Henri Lebesgue. We acknowledge the support of Pôle d'excellence cyber and GDR Sécurité Informatique in publicizing the workshop. The program ran very smoothly, for which we are indebted to Sylvain

Duquesne for his handling of the software platform SVI esolutions and for the tireless support he offered to each and everyone who had to use the platform.

As with the previous workshops, Springer agreed to publish the proceedings of WAIFI 2020 as an LNCS volume. We thank Alfred Hoffman and Anna Kramer at Springer for all their help. The EasyChair conference management system was helpful, once again, during submission and selection phases.

With almost no prior experience in organizing online workshops of this size, it was challenging at times to put together this event. Over 100 emails per week, exchanged between the (general, PC, publicity) chairs, organizing committee, authors, speakers, PC members and session chairs, especially during the weeks leading to the meeting, may indicate the indispensable support and understanding we received from all. We express our gratitude to them and all the participants of WAIFI 2020.

November 2020

Alev Topuzoğlu
Jean Claude Bajard

Organization

General Chairs

Sylvain Duquesne	IRMAR, Rennes 1, France
Arnaud Tisserand	CNRS, Lab-STICC, Lorient, France

Program Committee Chairs

Jean Claude Bajard	Sorbonne Université, France
Alev Topuzoğlu	Sabancı University, Turkey

Publicity Chair

José Luis Imaña	Complutense University of Madrid, Spain

Steering Committee

Lilya Budaghyan	University of Bergen, Norway
Claude Carlet	University of Paris 8, France
Anwar Hasan	University of Waterloo, Canada
José Luis Imaña	Complutense University of Madrid, Spain
Çetin Kaya Koç	University of California Santa Barbara, USA
Sihem Mesnager	University of Paris 8, France
Ferruh Özbudak	Middle East Technical University, Turkey
Svetla Petkova-Nikova	KU Leuven, Belgium
Francisco Rodríguez-Henríquez	CINVESTAV-IPN, Mexico
Erkay Savaş	Sabancı University, Turkey

Program Committee

Nurdagül Anbar	Sabancı University, Turkey
Diego Aranha	Aarhus University, Denmark
Lejla Batina	Radboud University, The Netherlands
Peter Beelen	Technical University of Denmark, Denmark
Karim Bigou	Université de Bretagne Occidentale, Brest, France
Joppe Bos	NXP Semiconductors, Leuven, Belgium
Claude Carlet	University of Paris 8, France
Robert Coulter	University of Delaware, USA
Massimo Giulietti	University of Perugia, Italy
Guang Gong	University of Waterloo, Canada
Robert Granger	University of Surrey, UK

Aurore Guillevic	Inria Nancy - Grand Est, France
Daniel Katz	California State University, Northridge, USA
Yinan Kong	Macquarie University, Australia
Gohar Kyureghyan	University of Rostock, Germany
Sihem Mesnager	University of Paris 8, France
Lucia Moura	University of Ottawa, Canada
Daniel Panario	Carleton University, Canada
Thomas Plantard	University of Wollongong, Australia
Alexander Pott	Otto von Guericke University Magdeburg, Germany
John Sheekey	University College of Dublin, Ireland
Antonia Wachter-Zeh	Technical University of Munich, Germany
Arne Winterhof	Johann Radon Institute for Computational and Applied Mathematics, Austria

Organizing Committee

Elisa Lorenzo Garcìa	IRMAR, Rennes 1, France
Felix Ulmer	IRMAR, Rennes 1, France
Pierre-Alain Fouque	IRISA, Rennes 1, France
Adeline Roux-Langlois	IRISA, Rennes 1, France
Karim Bigou	Université de Bretagne Occidentale, Brest, France

Additional Reviewers

Juliano Bandeira Lima
Daniele Bartoli
Matteo Bonini
Cunsheng Ding
Masaya Fujisawa
Amparo Fúster-Sabater
Anna-Maurin Graner
Somphong Jitman
Lukas Kölsch
Giorgos Kapetanakis
Frieder Ladisch
Stefano Lia
Petr Lisonek
Georg Maringer
Bruno Martin
Maria Montanucci
Alessandro Neri
Ferruh Özbudak
Marco Timpanella
Peter Schwabe
Arnaud Sipasseuth
Pietro Speziali
Qiang Wang
Zilong Wang
Giovanni Zini
Vincent Zucca

Abstracts of Invited Talks/Papers

Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra

Alessio Caminata[1] and Elisa Gorla[2]

[1] Dipartimento di Matematica, Università degli Studi di Genova, via Dodecaneso 35, 16146, Genova, Italy
caminata@dima.unige.it
[2] Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, 2000, Neuchâtel, Switzerland
elisa.gorla@unine.ch

Abstract. The complexity of computing the solutions of a system of multivariate polynomial equations by means of Gröbner bases computations is upper bounded by a function of the solving degree. In this paper, we discuss how to rigorously estimate the solving degree of a system, focusing on systems arising within public-key cryptography. In particular, we show that it is upper bounded by, and often equal to, the Castelnuovo-Mumford regularity of the ideal generated by the homogenization of the equations of the system, or by the equations themselves in case they are homogeneous. We discuss the underlying commutative algebra and clarify under which assumptions the commonly used results hold. In particular, we discuss the assumption of being in generic coordinates (often required for bounds obtained following this type of approach) and prove that systems that contain the field equations or their fake Weil descent are in generic coordinates. We also compare the notion of solving degree with that of degree of regularity, which is commonly used in the literature. We complement the paper with some examples of bounds obtained following the strategy that we describe.

Linearized Polynomials and Their Adjoints, and Some Connections to Linear Sets and Semifields

Gary McGuire and John Sheekey

UCD School of Mathematics and Statistics,
University College Dublin, Dublin, Ireland
gary.mcguire@ucd.ie
john.sheekey@ucd.ie

Abstract. For a q-linearized polynomial function L on a finite field, we give a new short proof of a known result, that $L(x)/x$ and $L^*(x)/x$ have the same image, where $L^*(x)$ denotes the adjoint of L. We give some consequences for semifields, recovering results first proved by Lavrauw and Sheekey. We also give a characterization of planar functions.

Efficient, Actively Secure MPC with a Dishonest Majority: a Survey

Emmanuela Orsi

imec-COSIC, KU Leuven,
Leuven, Belgium
emmanuela.orsini@kuleuven.be

Abstract. The last ten years have seen a tremendous growth in the interest and practicality of secure multiparty computation (MPC) and its possible applications. Secure MPC is indeed a very hot research topic and recent advances in the field have already been translated into commercial products world-wide. A major pillar in this advance has been in the case of active security with a dishonest majority, mainly due to the SPDZ-line of work protocols. This survey gives an overview of these protocols, with a focus of the original SPDZ paper (Damgård et al. CRYPTO 2012) and its subsequent optimizations.

Introduction to Quantum Computing

André Chailloux

Inria Paris, France

Abstract. The goal of this invited talk was to present an introduction to Quantum Computing for computer scientists which are *not specialists* in the field. Here we present a brief summary of the contents of this talk, available at http://www-labsticc.univ-ubs.fr/waifi2020/videos/waifi2020-video-plenary-chailloux.mp4.

After a small introduction to the field, the talk is divided into 4 parts: basic notions of quantum computing, quantum error correction, quantum algorithms and perspectives.

Basic Notions of Quantum Computing. I first present textbook knowledge on the foundations of Quantum Computing. Here, bits are replaced by qubits which can be represented by vectors in a complex Hilbert space, and computational gates are replaced by unitary matrices that act on these qubits. The talk goes through these notions not only by describing the mathematical rules behind quantum bits and operations but also trying to give an intuition behind fundamental notions of quantum computing: what does it mean to be in a superposition of states? What does it mean that measuring a state alters it?

Quantum Error Correction. I then briefly mention one important theorem: the Threshold Theorem. Qubits are indeed very fragile and become noisy very fast. There are ways to perform quantum error correction but this requires adding more qubits, which themselves create more errors. The Threshold Theorem states that it is possible to correct these errors faster than they occur when adding new qubits, so stable quantum computations are in theory possible, even though they require much more resources than those we have today.

Quantum Algorithms. Then, I present some of the most iconic quantum algorithms: Shor's algortihm and Grover's algorithm. Shor's quantum algorithm shows that with a fully working quantum computer, one can solve the factoring and the discrete logarithm problems in polynomial time. As a consequence, this would break most of today's public key cryptography and we need to design new public key cryptosystems if we want to avoid this weakness.

Perspectives for Quantum Computing. Finally, I present existing technologies for quantum computing and those we can expect in the near and less near future. Quantum Key Distribution for performing unconditional key exchange is a mature technology that is already commercially available and can be used for highly sensitive data. On the other hand, quantum computers are still at a very early stage. Very recently however, several private companies managed to construct small quantum computers that have up to around 60 qubits. While we can't perform any useful computation with these, we arrived at a point where these small quantum computers cannot be simulated with usual computers so there is indeed some strong computational power here that needs to be further improved in order to see real speedups promised by quantum computing.

Contents

Special Functions over Finite Fields

Bases