CONTEMPORARY MATHEMATICS

642

# Algebra for Secure and Reliable Communication Modeling

CIMPA Research School and Conference
Algebra for Secure and Reliable Communication Modeling
October 1–13, 2012
Morelia, State of Michoacán, Mexico

Mustapha Lahyane
Edgar Martínez-Moro
Editors


American Mathematical Society
Real Sociedad Matemática Española


American Mathematical Society

# Algebra for Secure and Reliable Communication Modeling

# CONTEMPORARY MATHEMATICS

**642**

# Algebra for Secure and Reliable Communication Modeling

CIMPA Research School and Conference
Algebra for Secure and Reliable Communication Modeling
October 1–13, 2012
Morelia, State of Michoacán, Mexico

Mustapha Lahyane
Edgar Martínez-Moro
Editors


American Mathematical Society
Real Sociedad Matemática Española


**American Mathematical Society**
Providence, Rhode Island

2010 *Mathematics Subject Classification*. Primary 11T71, 14G50, 14Q05.

The photographs on p. xiii are reprinted with permission.

**Library of Congress Cataloging-in-Publication Data**

Algebra for secure and reliable communication modeling : CIMPA Research School and Conference on Algebra and Geometry for Reliable Communication Modeling, October 1–13, 2012, Morelia, state of Michoacán, Mexico / Mustapha Lahyane, Edgar Martinez-Moro, editors.

pages cm. – (Contemporary mathematics ; volume 642)
Includes bibliographical references.
ISBN 978-1-4704-1018-6 (alk. paper)
1. Signal processing–Mathematics–Congresses. 2. Geometry, Algebraic–Congresses. I. Lahyane, Mustapha, 1967– editor. II. Martínez-Moro, Edgar, editor.
TK5102.9.A42 2015
621.382′20151274–dc23  2014047010

Contemporary Mathematics ISSN: 0271-4132 (print); ISSN: 1098-3627 (online)

DOI: http://dx.doi.org/10.1090/conm/642

Dedicated to Alan Mathison Turing on the
50th anniversary of his death.

## Contents

# Preface

This volume contains the proceedings of the CIMPA Research School and Conference on Algebra for Secure and Reliable Communication Modeling, held in Morelia, State of Michoacán, Mexico from October 1–13, 2012.

The aim of the ASReCoM school and conference was to fill in the gap between the theoretical part of algebraic geometry and the applications to problem solving and computational modeling in engineering, signal processing and information theory. This involves nontrivial knowledge of algebra and geometry. The students at this CIMPA school received both theoretical and practical insight in those topics, and as is traditional in modeling schools, also in the software needed to deal with modeling problems.

The authors involved with this volume have written self-contained papers on some of the most important and current topics in coding theory. The papers are based on lectures given at the AsReCom CIMPA School. The authors were asked to take special care in pointing out possible research lines as well as possible applications of the theoretical algebraic background. Each paper has a carefully selected list of references of the most outstanding papers on the topic. All the papers have been fully refereed according to the "Contemporary Mathematics" high standards. We are very grateful to the referees for their assistance in helping us put together such a nice volume.

We have included contributions on several aspects of coding theory gathered into three categories: (i) General theory of linear codes (the first two papers); (ii) Algebraic geometry and coding theory (papers 3–7); and (iii) Constacyclic codes over finite fields and rings (papers 8–9).

We would like to thank sincerely (in alphabetical order) the following for the financial assistance and support they provided to us before and during the school and the conference: Comité Académico Conjunto (CAC) del Posgrado Conjunto en Ciencias Matemáticas UNAM-UMSNH, the Consejo Estatal de Ciencia, Tecnología e Innovación de Michoacán (CECTI), the Coordinación de Investigación Científica de la Universidad Michoacana de San Nicolás de Hidalgo, the International Center for Pure and Applied Mathematics (CIMPA), the International Mathematical Union (IMU), the Instituto de Física y Matemáticas de la Universidad Michoacana de San Nicolás de Hidalgo, the Office of External Activities (OEA) of The Abdus Salam International Centre for Theoretical Physics (ICTP), the Secretaría Académica de la Universidad Michoacana de San Nicolás de Hidalgo, the University of Valladolid (UVa), and the Universidad Jaume I (UJI). Without their help our project would have never seen the light of day.

Many thanks go to Christian Mauduit, Claude Cibils, Luis Manual Villaseñor Cendejas, Esther García Garibay, Brenda Leticia De La Rosa Navarro, Juan Bosco

Frías Medina, Oscar Sánchez Reyes, Candy Pompa, Israel Moreno Mejía, Jorge Olivares Vázquez, Thibault Rousseau, Osvaldo Osuna Castro, V. Janitzio Mejía Huguet, Gerardo Tinoco Ruiz, Medardo Serna González, and Ricardo Becerril Bárcenas.

Finally we also want to thank Pedro José Paúl Escolano for all his help with the editorial process.

Mustapha Lahyane
Edgar Martínez-Moro
October 2014

## List of Participants

Naila Itzel Angelina Centeno
University of Michoacán, Mexico

Cicero Carvalho
Universidade Federal de Uberlandia, Brazil

Christian Eduardo Castillo Valadez
University of Michoacán, Mexico

Jesús Adrián Cerda Rodríguez
University of Michoacán, Mexico

Michela Ceria
University of Turin, Italy

María de los Angeles Chara
Instituto de Matemática Aplicada del Litoral, Argentina

Henry Ricardo de Jesús Chimal Dzul
Universidad Autónoma Metropolitana, Mexico

Brenda Leticia De La Rosa Navarro
University of Michoacán, Mexico

Hai Quang Dinh
Kent State University, USA

José Ignacio Farrán Martín
University of Valladolid, Spain

Juan Bosco Frías Medina
University of Michoacán, Mexico

Carlos Galindo Pastor
University of Jaume I, Spain

Arturo E. Giles Flores
Center of Investigations in Mathematics (CIMAT), Mexico

Mustapha Lahyane
University of Michoacán, Mexico

Hiram Habid López Valdez
CINVESTAV, Mexico

Irene Márquez Corbella
University of Valladolid, Spain

Edgar Martínez Moro
University of Valladolid, Spain

Christian Mauduit
Universite da Aix-Marseille I (Universite de Provence), France

Wilfredo Morales Lezca
Universidad de la Habana, Cuba

Israel Moreno Mejía
National Autonomous University of Mexico, Mexico

Carlos Munuera Gómez
University of Valladolid, Spain

Wilson Olaya León
Universidad Industrial de Santander, Colombia

Carlos Osvaldo Osuna Castro
University of Michoacán, Mexico

Emma Previato
Boston University, USA

Luciane Quoos Conte
Universidade Federal do Rio de Janeiro, Brazil

Vither Franco Rojas Tarquino
University of Michoacán, Mexico

Oscar Sánchez Reyes
University of Michoacán, Mexico

Alonso Sepúlveda Castellanos
Universidade Federal do Rio de Janeiro,
Brazil

Verónica Suaste
Center of Investigations in Mathematics
(CIMAT), Mexico

Guilherme Tizziotti
Universidade Federal de Uberlandia,
Brazil

Laurence Emilie Um
Mohammed V University, Morocco

Juan Fernando Valdés Cruz
Universidad del Valle de Guatemala,
Guatemala

Jay A. Wood
Western Michigan University, USA


**Break and informal conversation during the first week**


**Group excursion (Second week)**

# Selected Published Titles in This Series

642 **Mustapha Lahyane and Edgar Martínez-Moro, Editors,** Algebra for Secure and Reliable Communication Modeling, 2015

638 **Javad Mashreghi, Emmanuel Fricain, and William Ross, Editors,** Invariant Subspaces of the Shift Operator, 2015

637 **Stéphane Ballet, Marc Perret, and Alexey Zaytsev, Editors,** Algorithmic Arithmetic, Geometry, and Coding Theory, 2015

636 **Simeon Reich and Alexander J. Zaslavski, Editors,** Infinite Products of Operators and Their Applications, 2015

635 **Christopher W. Curtis, Anton Dzhamay, Willy A. Hereman, and Barbara Prinari, Editors,** Nonlinear Wave Equations, 2015

634 **Steven Dougherty, Alberto Facchini, André Leroy, Edmund Puczyłowski, and Patrick Solé, Editors,** Noncommutative Rings and Their Applications, 2015

633 **Delaram Kahrobaei and Vladimir Shpilrain, Editors,** Algorithmic Problems of Group Theory, Their Complexity, and Applications to Cryptography, 2015

632 **Gohar Kyureghyan, Gary L. Mullen, and Alexander Pott, Editors,** Topics in Finite Fields, 2015

631 **Siddhartha Bhattacharya, Tarun Das, Anish Ghosh, and Riddhi Shah, Editors,** Recent Trends in Ergodic Theory and Dynamical Systems, 2015

630 **Pierre Albin, Dmitry Jakobson, and Frédéric Rochon, Editors,** Geometric and Spectral Analysis, 2014

629 **Milagros Izquierdo, S. Allen Broughton, Antonio F. Costa, and Rubí E. Rodríguez, Editors,** Riemann and Klein Surfaces, Automorphisms, Symmetries and Moduli Spaces, 2014

628 **Anita T. Layton and Sarah D. Olson, Editors,** Biological Fluid Dynamics: Modeling, Computations, and Applications, 2014

627 **Krishnaswami Alladi, Frank Garvan, and Ae Ja Yee, Editors,** Ramanujan 125, 2014

626 **Veronika Furst, Keri A. Kornelson, and Eric S. Weber, Editors,** Operator Methods in Wavelets, Tilings, and Frames, 2014

625 **Alexander Barg and Oleg R. Musin, Editors,** Discrete Geometry and Algebraic Combinatorics, 2014

624 **Karl-Dieter Crisman and Michael A. Jones, Editors,** The Mathematics of Decisions, Elections, and Games, 2014

623 **Pramod N. Achar, Dijana Jakelić, Kailash C. Misra, and Milen Yakimov, Editors,** Recent Advances in Representation Theory, Quantum Groups, Algebraic Geometry, and Related Topics, 2014

622 **S. Ejaz Ahmed, Editor,** Perspectives on Big Data Analysis, 2014

621 **Ludmil Katzarkov, Ernesto Lupercio, and Francisco J. Turrubiates, Editors,** The Influence of Solomon Lefschetz in Geometry and Topology, 2014

620 **Ulrike Tillmann, Søren Galatius, and Dev Sinha, Editors,** Algebraic Topology: Applications and New Directions, 2014

619 **Gershon Wolansky and Alexander J. Zaslavski, Editors,** Variational and Optimal Control Problems on Unbounded Domains, 2014

618 **Abba B. Gumel, Editor,** Mathematics of Continuous and Discrete Dynamical Systems, 2014

617 **Christian Ausoni, Kathryn Hess, Brenda Johnson, Wolfgang Lück, and Jérôme Scherer, Editors,** An Alpine Expedition through Algebraic Topology, 2014

616 **G. L. Litvinov and S. N. Sergeev, Editors,** Tropical and Idempotent Mathematics and Applications, 2014

For a complete list of titles in this series, visit the
AMS Bookstore at **www.ams.org/bookstore/conmseries/**.

CONM 642

ASReCoM • Lahyane et al., Editors

This volume contains the proceedings of the CIMPA Research School and Conference on Algebra for Secure and Reliable Communication Modeling, held from October 1–13, 2012, in Morelia, State of Michoacán, Mexico.

The papers cover several aspects of the theory of coding theory and are gathered into three categories: general theory of linear codes, algebraic geometry and coding theory, and constacyclic codes over rings.

The aim of this volume is to fill the gap between the theoretical part of algebraic geometry and the applications to problem solving and computational modeling in engineering, signal processing and information theory.

American Mathematical Society
**www.ams.org**

Real Sociedad Matemática Española
**www.rsme.es**

ISBN 978-1-4704-1018-6

9 781470 410186

CONM/642

AMS/RSME