CONTEMPORARY MATHEMATICS

724

# Algebraic Curves and Their Applications

Lubjana Beshaj
Tony Shaska
Editors

AMS American Mathematical Society

# Algebraic Curves and Their Applications

CONTEMPORARY MATHEMATICS

724

# Algebraic Curves and Their Applications

Lubjana Beshaj
Tony Shaska
Editors

AMS American Mathematical Society

2010 *Mathematics Subject Classification.* Primary 11G30, 11G50, 11G32, 11T71, 11T06, 14H37, 14H40, 14H45, 14H52, 14H55.

---

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

Names: Beshaj, Lubjana, 1986- editor. | Shaska, Tony, 1967- editor.
Title: Algebraic curves and their applications / Lubjana Beshaj, Tony Shaska Editors.
Description: Providence, Rhode Island : American Mathematical Society, [2019] | Series: Contemporary mathematics ; volume 724 | Includes bibliographical references.
Identifiers: LCCN 2018040058 | ISBN 9781470442477 (alk. paper)
Subjects: LCSH: Curves, Algebraic.
Classification: LCC QA565 .A447 2019 | DDC 516.3/52–dc23
LC record available at https://lccn.loc.gov/2018040058

DOI: https://doi.org/10.1090/conm/724

---

## Contents

# Preface

Algebraic curves are one of the most classical objects in mathematics. Their study led to the development of many branches of mathematics, such as invariant theory, Riemann surfaces, and algebraic geometry, with some of the biggest names in mathematics, such as Abel, Jacobi, Riemann, Weierstrass, and Noether, contributing to a beautiful theory and laying the foundation for what is known today as modern algebraic geometry.

In the last few decades, with the development of computational techniques and the significant growth in computer power, algebraic curves have found many applications, most notably in algebraic coding theory, cryptography, and dynamical systems. The goal of this book is to focus on such applications.

This volume consists of a variety of papers that combine classical questions on algebraic curves with more recent developments and applications. While some of the papers are long surveys covering such topics as automorphisms of algebraic curves, Abelian and Jacobian varieties, and cryptography, other papers are focused on new trends, such as tropical geometry, arithmetic statistics of the moduli space of curves, and applications of curves to differential equations. Below we briefly describe each contribution.

Bekker and Zarhin study families of elliptic curves with rational torsion points of even order. They construct explicitly versal families of elliptic curves with rational points of order 4, 6, 8, 10, and 12, respectively. They also construct versal families of elliptic curves in characteristic 2 that admit a rational point of order 4 or 8.

Beshaj and Guest study the weighted moduli spaces of sextics. This is a continuation of a series of papers on the distribution of points in the moduli space of genus two for which the field of moduli is not a field of definition. In this paper, they use the weighted moduli height to investigate the distribution of fine moduli points in the moduli space of genus two curves. They show that for any genus two curve with equation $y^2 = f(x)$, its weighted moduli height is $\mathfrak{h}(\mathfrak{p}) \leq 2^3\sqrt{3 \cdot 5 \cdot 7} \cdot H(f)$, where $H(f)$ is the minimal naive height of the curve. Based on the weighted moduli height $\mathfrak{h}$, they create a database of genus two curves defined over $\mathbb{Q}$ with small $\mathfrak{h}$ and show that for small such height ($\mathfrak{h} < 5$) about 30% of points are fine moduli points.

Ford studies a family of non-normal double planes associated to hyperelliptic curves. He generalizes the construction of a non-normal rational affine double plane $X \to \mathbb{A}^2_k$ together with a one-to-one homomorphism from the subgroup of torsion elements in the Picard group of $C$ to the Brauer group of $X$ to the situation where $C$ is an arbitrary affine variety.

Otake and Shaska study the discriminant of certain quadrinomials. They give an explicit formula for the discriminant $\Delta_f(x)$ of the quadrinomials of the form $f(x) = x^n + t(x^2 + ax + b)$. The proof uses Bezoutians of polynomials. This extends the work of Selmer, Mori, and others.

Dokchitser, Dokchitser, Maistret, and Morgan explore three combinatorial descriptions of semistable types of hyperelliptic curves over local fields: dual graphs, their quotient trees by the hyperelliptic involution, and configurations of the roots of the defining equation ("cluster pictures"). They construct explicit combinatorial one-to-one correspondences between the three, which furthermore respect automorphisms and allow one to keep track of the monodromy pairing and the Tamagawa group of the Jacobian. They introduce a classification scheme and a naming convention for semistable types of hyperelliptic curves and types with a Frobenius action. This is the higher genus analogue of the distinction between good, split, and non-split multiplicative reduction for elliptic curves.

Stout studies formal deformations of algebraic spaces and generalizations of the motivic Igusa-zeta function. He generalizes the notion of the auto-Igusa-zeta function to formal deformations of algebraic spaces. By incorporating data from all algebraic transformations of local coordinates, this function can be viewed as a generalization of the traditional motivic Igusa-zeta function. Furthermore, the author introduces a new series, which he calls the canonical auto-Igusa-zeta function, whose coefficients are given by the quotient stacks formed from the coefficients of the auto-Igusa-zeta function modulo change of coordinates.

Mandili and Shaska study computing heights on weighted projective spaces. They extend the concept of height on projective spaces to that of weighted height on weighted projective spaces and show the basic properties of this height and how it can be used to study hyperelliptic/superelliptic curves. Some examples are provided from the weighted moduli space of binary sextics and octavics.

Beshaj and Polak study the moduli space of genus three hyperelliptic curves via the weighted projective space of binary octavics. This enables them to create a database of genus three hyperelliptic curves of weighted moduli height $\mathfrak{h} = 1$. Genus three hyperelliptic curves are some of the most interesting curves in cryptography due to the many interesting properties of their Jacobians. It is the first time that a database on such curves is compiled and organized.

Broughton, Shaska, and Wootton give a complete survey of automorphism groups of algebraic curves defined over a field $F$ of characteristic $p \geq 0$. This is a classical problem with a rich and beautiful history with many notable mathematicians involved, such as Klein, Friecke, Wimann, Hurwitz, MacBeath, Accola, Singerman, and Stichtenoth. The paper gives a comprehensive review of the main results in zero characteristic and in positive characteristic. They display complete tables of groups for all characteristics for genus $g = 3$ and $g = 4$ and give algorithms for how this can be done for any genus. This paper will be valuable for many mathematicians who work in the area and want a single source for automorphisms of algebraic curves. Several open problems are suggested throughout the paper.

Cortázar and Costa study the algebraic classification of subgroups of hyperbolic planar crystallographic groups. A planar Euclidean or hyperbolic crystallographic group $\Delta$ is a subgroup of the group of isometries of the Euclidean plane $\mathbb{E}^2$, respectively, the hyperbolic plane $\mathbb{H}^2$, with compact orbit space. These groups are classified algebraically by a symbol called signature and an equivalence relation

defined on the set of signatures. In 1990, A. H. M. Hoare gave an algorithm to obtain the signature of a finite index subgroup of a planar crystallographic group. Recently, authors Cortázar and Costa completed the algorithm of Hoare and implemented it in GAP.

Bujalance, Conder, Costa, and Izquierdo study regular dessins d'enfants with $4g$ automorphisms and Wiman's curve. They show that with a few exceptions, every regular dessin d'enfant with genus $g$ having exactly $4g$ automorphisms is embedded in Wiman's curve of type II.

Hidalgo studies an explicit descent of real algebraic varieties. In this paper, he gives an explicit method on how to compute the equations for real algebraic varieties. The main tools used by the author are provided by the theory of fields of moduli and fields of definition. The method used is a consequence of Weil's descent theorem.

Previato focuses on curves on isomonodromy and isospectral deformations: Painlevé VI as a case study. Certain integrable dynamical problems can be described by isospectral deformations; under certain restrictions, the spectrum is an algebraic curve. On the other hand, certain isomonodromy deformations may have an associated algebraic curve, under certain restrictions on the monodromy group. This manuscript is a survey of the study on the relation between isomonodromy and isospectral deformations. The author shows a non-trivial result of the problem in Benes and Previato [J. Phys. A 43 (2010), 434006, 14 pp.] and, based on the result, shows the current state of the investigations of the relation.

Boston and Hao introduce a family of codes called *quasi-quadratic residuecodes* in algebraic coding theory. These codes are interesting because their weight distributions play an important role in a famous conjecture in coding theory known as *Goppa's conjecture*. Furthermore, the weight of their codewords has a close relation with the number of points on corresponding hyperelliptic curves. In the second part, they implement a heuristic model to estimate the limiting behavior of the number of points on related hyperelliptic curves over $\mathbb{F}_p$ as $p$ goes to infinity. For primes $p < 50$, explicit calculations are given. These results provide evidence that Goppa's conjecture is dubious.

Frey and Shaska give the latest developments in the theory of curves, Jacobians, and cryptography. In the first part, they provide the necessary mathematical background on Abelian varieties, their torsion points, Honda-Tate theory, and Galois representations, with emphasis on Jacobian varieties and hyperelliptic Jacobians. In the second part, they focus on applications of Abelian varieties in cryptography and treat separately elliptic curve cryptography and genus two and three cryptography, including Diffie-Hellman key exchange, index calculus in Picard groups, isogenies of Jacobians via correspondences, and applications to discrete logarithms. Several open problems and new directions are suggested.

We hope this book will be helpful to all mathematicians working with algebraic curves, especially those who are crossing over from other areas of mathematics. Special thanks to all of the authors who contributed papers, the referees for all of their work and effort, and the AMS production staff for their help in preparing this book.

Lubjana Beshaj and Tony Shaska

# Selected Published Titles in This Series

724 **Lubjana Beshaj and Tony Shaska, Editors,** Algebraic Curves and Their Applications, 2019

720 **Alexandre Girouard, Editor,** Spectral Theory and Applications, 2018

719 **Florian Sobieczky, Editor,** Unimodularity in Randomly Generated Graphs, 2018

718 **David Ayala, Daniel S. Freed, and Ryan E. Grady, Editors,** Topology and Quantum Theory in Interaction, 2018

717 **Federico Bonetto, David Borthwick, Evans Harrell, and Michael Loss, Editors,** Mathematical Problems in Quantum Physics, 2018

716 **Alex Martsinkovsky, Kiyoshi Igusa, and Gordana Todorov, Editors,** Surveys in Representation Theory of Algebras, 2018

715 **Sergio R. López-Permouth, Jae Keol Park, S. Tariq Rizvi, and Cosmin S. Roman, Editors,** Advances in Rings and Modules, 2018

714 **Jens Gerlach Christensen, Susanna Dann, and Matthew Dawson, Editors,** Representation Theory and Harmonic Analysis on Symmetric Spaces, 2018

713 **Naihuan Jing and Kailash C. Misra, Editors,** Representations of Lie Algebras, Quantum Groups and Related Topics, 2018

712 **Nero Budur, Tommaso de Fernex, Roi Docampo, and Kevin Tucker, Editors,** Local and Global Methods in Algebraic Geometry, 2018

711 **Thomas Creutzig and Andrew R. Linshaw, Editors,** Vertex Algebras and Geometry, 2018

710 **Raphaël Danchin, Reinhard Farwig, Jiří Neustupa, and Patrick Penel, Editors,** Mathematical Analysis in Fluid Mechanics, 2018

709 **Fernando Galaz-García, Juan Carlos Pardo Millán, and Pedro Solórzano, Editors,** Contributions of Mexican Mathematicians Abroad in Pure and Applied Mathematics, 2018

708 **Christian Ausoni, Kathryn Hess, Brenda Johnson, Ieke Moerdijk, and Jérôme Scherer, Editors,** An Alpine Bouquet of Algebraic Topology, 2018

707 **Nitya Kitchloo, Mona Merling, Jack Morava, Emily Riehl, and W. Stephen Wilson, Editors,** New Directions in Homotopy Theory, 2018

706 **Yeonhyang Kim, Sivaram K. Narayan, Gabriel Picioroaga, and Eric S. Weber, Editors,** Frames and Harmonic Analysis, 2018

705 **Graham J. Leuschke, Frauke Bleher, Ralf Schiffler, and Dan Zacharia, Editors,** Representations of Algebras, 2018

704 **Alain Escassut, Cristina Perez-Garcia, and Khodr Shamseddine, Editors,** Advances in Ultrametric Analysis, 2018

703 **Andreas Malmendier and Tony Shaska, Editors,** Higher Genus Curves in Mathematical Physics and Arithmetic Geometry, 2018

702 **Mark Grant, Gregory Lupton, and Lucile Vandembroucq, Editors,** Topological Complexity and Related Topics, 2018

701 **Joan-Carles Lario and V. Kumar Murty, Editors,** Number Theory Related to Modular Curves, 2018

700 **Alexandre Girouard, Dmitry Jakobson, Michael Levitin, Nilima Nigam, Iosif Polterovich, and Frédéric Rochon, Editors,** Geometric and Computational Spectral Theory, 2017

699 **Mark L. Agranovsky, Matania Ben-Artzi, Catherine Bénéteau, Lavi Karp, Dmitry Khavinson, Simeon Reich, David Shoikhet, Gilbert Weinstein, and Lawrence Zalcman, Editors,** Complex Analysis and Dynamical Systems VII, 2017

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

CONM 724

# Algebraic Curves • Beshaj and Shaska, Editors

This volume contains a collection of papers on algebraic curves and their applications. While algebraic curves traditionally have provided a path toward modern algebraic geometry, they also provide many applications in number theory, computer security and cryptography, coding theory, differential equations, and more.

Papers cover topics such as the rational torsion points of elliptic curves, arithmetic statistics in the moduli space of curves, combinatorial descriptions of semistable hyperelliptic curves over local fields, heights on weighted projective spaces, automorphism groups of curves, hyperelliptic curves, dessins d'enfants, applications to Painlevé equations, descent on real algebraic varieties, quadratic residue codes based on hyperelliptic curves, and Abelian varieties and cryptography.

This book will be a valuable resource for people interested in algebraic curves and their connections to other branches of mathematics.

AMS
www.ams.org

ISBN 978-1-4704-4247-7

9 781470 442477

CONM/724

AMS