LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor N.J. Hitchin, Mathematical Institute,
University of Oxford, 24–29 St Giles, Oxford OX1 3LB, United Kingdom

The titles below are available from booksellers, or, in case of difficulty, from Cambridge University Press.

90 Polytopes and symmetry, S.A. ROBERTSON
96 Diophantine equations over function fields, R.C. MASON
97 Varieties of constructive mathematics, D.S. BRIDGES & F. RICHMAN
99 Methods of differential geometry in algebraic topology, M. KAROUBI & C. LERUSTE
100 Stopping time techniques for analysts and probabilists, L. EGGHE
104 Elliptic structures on 3-manifolds, C.B. THOMAS
105 A local spectral theory for closed operators, I. ERDELYI & WANG SHENGWANG
107 Compactification of Siegel moduli schemes, C.-L. CHAI
109 Diophantine analysis, J. LOXTON & A. VAN DER POORTEN (eds)
113 Lectures on the asymptotic theory of ideals, D. REES
116 Representations of algebras, P.J. WEBB (ed)
119 Triangulated categories in the representation theory of finite-dimensional algebras, D. HAPPEL
121 Proceedings of *Groups - St Andrews 1985*, E. ROBERTSON & C. CAMPBELL (eds)
128 Descriptive set theory and the structure of sets of uniqueness, A.S. KECHRIS & A. LOUVEAU
130 Model theory and modules, M. PREST
131 Algebraic, extremal & metric combinatorics, M.-M. DEZA, P. FRANKL & I.G. ROSENBERG (eds)
138 Analysis at Urbana, II, E. BERKSON, T. PECK, & J. UHL (eds)
139 Advances in homotopy theory, S. SALAMON, B. STEER & W. SUTHERLAND (eds)
140 Geometric aspects of Banach spaces, E.M. PEINADOR & A. RODES (eds)
141 Surveys in combinatorics 1989, J. SIEMONS (ed)
144 Introduction to uniform spaces, I.M. JAMES
146 Cohen-Macaulay modules over Cohen-Macaulay rings, Y. YOSHINO
148 Helices and vector bundles, A.N. RUDAKOV *et al*
149 Solitons, nonlinear evolution equations and inverse scattering, M. ABLOWITZ & P. CLARKSON
150 Geometry of low-dimensional manifolds 1, S. DONALDSON & C.B. THOMAS (eds)
151 Geometry of low-dimensional manifolds 2, S. DONALDSON & C.B. THOMAS (eds)
152 Oligomorphic permutation groups, P. CAMERON
153 L-functions and arithmetic, J. COATES & M.J. TAYLOR (eds)
155 Classification theories of polarized varieties, TAKAO FUJITA
158 Geometry of Banach spaces, P.F.X. MÜLLER & W. SCHACHERMAYER (eds)
159 Groups St Andrews 1989 volume 1, C.M. CAMPBELL & E.F. ROBERTSON (eds)
160 Groups St Andrews 1989 volume 2, C.M. CAMPBELL & E.F. ROBERTSON (eds)
161 Lectures on block theory, BURKHARD KÜLSHAMMER
163 Topics in varieties of group representations, S.M. VOVSI
164 Quasi-symmetric designs, M.S. SHRIKANDE & S.S. SANE
166 Surveys in combinatorics, 1991, A.D. KEEDWELL (ed)
168 Representations of algebras, H. TACHIKAWA & S. BRENNER (eds)
169 Boolean function complexity, M.S. PATERSON (ed)
170 Manifolds with singularities and the Adams-Novikov spectral sequence, B. BOTVINNIK
171 Squares, A.R. RAJWADE
172 Algebraic varieties, GEORGE R. KEMPF
173 Discrete groups and geometry, W.J. HARVEY & C. MACLACHLAN (eds)
174 Lectures on mechanics, J.E. MARSDEN
175 Adams memorial symposium on algebraic topology 1, N. RAY & G. WALKER (eds)
176 Adams memorial symposium on algebraic topology 2, N. RAY & G. WALKER (eds)
177 Applications of categories in computer science, M. FOURMAN, P. JOHNSTONE & A. PITTS (eds)
178 Lower K- and L-theory, A. RANICKI
179 Complex projective geometry, G. ELLINGSRUD *et al*
180 Lectures on ergodic theory and Pesin theory on compact manifolds, M. POLLICOTT
181 Geometric group theory I, G.A. NIBLO & M.A. ROLLER (eds)
182 Geometric group theory II, G.A. NIBLO & M.A. ROLLER (eds)
183 Shintani zeta functions, A. YUKIE
184 Arithmetical functions, W. SCHWARZ & J. SPILKER
185 Representations of solvable groups, O. MANZ & T.R. WOLF
186 Complexity: knots, colourings and counting, D.J.A. WELSH
187 Surveys in combinatorics, 1993, K. WALKER (ed)
188 Local analysis for the odd order theorem, H. BENDER & G. GLAUBERMAN
189 Locally presentable and accessible categories, J. ADAMEK & J. ROSICKY
190 Polynomial invariants of finite groups, D.J. BENSON
191 Finite geometry and combinatorics, F. DE CLERCK *et al*
192 Symplectic geometry, D. SALAMON (ed)
194 Independent random variables and rearrangement invariant spaces, M. BRAVERMAN
195 Arithmetic of blowup algebras, WOLMER VASCONCELOS
196 Microlocal analysis for differential operators, A. GRIGIS & J. SJÖSTRAND
197 Two-dimensional homotopy and combinatorial group theory, C. HOG-ANGELONI *et al*
198 The algebraic characterization of geometric 4-manifolds, J.A. HILLMAN
199 Invariant potential theory in the unit ball of $\mathbf{C}^n$, MANFRED STOLL
200 The Grothendieck theory of dessins d'enfant, L. SCHNEPS (ed)
201 Singularities, JEAN-PAUL BRASSELET (ed)
202 The technique of pseudodifferential operators, H.O. CORDES
203 Hochschild cohomology of von Neumann algebras, A. SINCLAIR & R. SMITH
204 Combinatorial and geometric group theory, A.J. DUNCAN, N.D. GILBERT & J. HOWIE (eds)

205 Ergodic theory and its connections with harmonic analysis, K. PETERSEN & I. SALAMA (eds)
207 Groups of Lie type and their geometries, W.M. KANTOR & L. DI MARTINO (eds)
208 Vector bundles in algebraic geometry, N.J. HITCHIN, P. NEWSTEAD & W.M. OXBURY (eds)
209 Arithmetic of diagonal hypersurfaces over finite fields, F.Q. GOUVÊA & N. YUI
210 Hilbert C*-modules, E.C. LANCE
211 Groups 93 Galway / St Andrews I, C.M. CAMPBELL *et al* (eds)
212 Groups 93 Galway / St Andrews II, C.M. CAMPBELL *et al* (eds)
214 Generalised Euler-Jacobi inversion formula and asymptotics beyond all orders, V. KOWALENKO *et al*
215 Number theory 1992–93, S. DAVID (ed)
216 Stochastic partial differential equations, A. ETHERIDGE (ed)
217 Quadratic forms with applications to algebraic geometry and topology, A. PFISTER
218 Surveys in combinatorics, 1995, PETER ROWLINSON (ed)
220 Algebraic set theory, A. JOYAL & I. MOERDIJK
221 Harmonic approximation, S.J. GARDINER
222 Advances in linear logic, J.-Y. GIRARD, Y. LAFONT & L. REGNIER (eds)
223 Analytic semigroups and semilinear initial boundary value problems, KAZUAKI TAIRA
224 Computability, enumerability, unsolvability, S.B. COOPER, T.A. SLAMAN & S.S. WAINER (eds)
225 A mathematical introduction to string theory, S. ALBEVERIO, J. JOST, S. PAYCHA, S. SCARLATTI
226 Novikov conjectures, index theorems and rigidity I, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
227 Novikov conjectures, index theorems and rigidity II, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
228 Ergodic theory of $\mathbb{Z}^d$ actions, M. POLLICOTT & K. SCHMIDT (eds)
229 Ergodicity for infinite dimensional systems, G. DA PRATO & J. ZABCZYK
230 Prolegomena to a middlebrow arithmetic of curves of genus 2, J.W.S. CASSELS & E.V. FLYNN
231 Semigroup theory and its applications, K.H. HOFMANN & M.W. MISLOVE (eds)
232 The descriptive set theory of Polish group actions, H. BECKER & A.S. KECHRIS
233 Finite fields and applications, S. COHEN & H. NIEDERREITER (eds)
234 Introduction to subfactors, V. JONES & V.S. SUNDER
235 Number theory 1993–94, S. DAVID (ed)
236 The James forest, H. FETTER & B. GAMBOA DE BUEN
237 Sieve methods, exponential sums, and their applications in number theory, G.R.H. GREAVES *et al*
238 Representation theory and algebraic geometry, A. MARTSINKOVSKY & G. TODOROV (eds)
239 Clifford algebras and spinors, P. LOUNESTO
240 Stable groups, FRANK O. WAGNER
241 Surveys in combinatorics, 1997, R.A. BAILEY (ed)
242 Geometric Galois actions I, L. SCHNEPS & P. LOCHAK (eds)
243 Geometric Galois actions II, L. SCHNEPS & P. LOCHAK (eds)
244 Model theory of groups and automorphism groups, D. EVANS (ed)
245 Geometry, combinatorial designs and related structures, J.W.P. HIRSCHFELD *et al*
246 p-Automorphisms of finite p-groups, E.I. KHUKHRO
247 Analytic number theory, Y. MOTOHASHI (ed)
248 Tame topology and o-minimal structures, LOU VAN DEN DRIES
249 The atlas of finite groups: ten years on, ROBERT CURTIS & ROBERT WILSON (eds)
250 Characters and blocks of finite groups, G. NAVARRO
251 Gröbner bases and applications, B. BUCHBERGER & F. WINKLER (eds)
252 Geometry and cohomology in group theory, P. KROPHOLLER, G. NIBLO, R. STÖHR (eds)
253 The q-Schur algebra, S. DONKIN
254 Galois representations in arithmetic algebraic geometry, A.J. SCHOLL & R.L. TAYLOR (eds)
255 Symmetries and integrability of difference equations, P.A. CLARKSON & F.W. NIJHOFF (eds)
256 Aspects of Galois theory, HELMUT VÖLKLEIN *et al*
257 An introduction to noncommutative differential geometry and its physical applications 2ed, J. MADORE
258 Sets and proofs, S.B. COOPER & J. TRUSS (eds)
259 Models and computability, S.B. COOPER & J. TRUSS (eds)
260 Groups St Andrews 1997 in Bath, I, C.M. CAMPBELL *et al*
261 Groups St Andrews 1997 in Bath, II, C.M. CAMPBELL *et al*
263 Singularity theory, BILL BRUCE & DAVID MOND (eds)
264 New trends in algebraic geometry, K. HULEK, F. CATANESE, C. PETERS & M. REID (eds)
265 Elliptic curves in cryptography, I. BLAKE, G. SEROUSSI & N. SMART
267 Surveys in combinatorics, 1999, J.D. LAMB & D.A. PREECE (eds)
268 Spectral asymptotics in the semi-classical limit, M. DIMASSI & J. SJÖSTRAND
269 Ergodic theory and topological dynamics, M.B. BEKKA & M. MAYER
270 Analysis on Lie Groups, N.T. VAROPOULOS & S. MUSTAPHA
271 Singular perturbations of differential operators, S. ALBEVERIO & P. KURASOV
272 Character theory for the odd order function, T. PETERFALVI
273 Spectral theory and geometry, E.B. DAVIES & Y. SAFAROV (eds)
274 The Mandelbrot set, theme and variations, TAN LEI (ed)
275 Computatoinal and geometric aspects of modern algebra, M. D. ATKINSON *et al* (eds)
276 Singularities of plane curves, E. CASAS-ALVERO
277 Descriptive set theory and dynamical systems, M. FOREMAN *et al* (eds)
278 Global attractors in abstract parabolic problems, J.W. CHOLEWA & T. DLOTKO
279 Topics in symbolic dynamics and applications, F. BLANCHARD, A. MAASS & A. NOGUEIRA (eds)
280 Characters and Automorphism Groups of Compact Riemann Surfaces, T. BREUER
281 Explicit birational geometry of 3-folds, ALESSIO CORTI & MILES REID (eds)
282 Auslander-Buchweitz approximations of equivariant modules, M. HASHIMOTO
283 Nonlinear elasticity, R. OGDEN & Y. FU (eds)
284 Foundations of computational mathematics, R. DEVORE, A. ISERLES, E. SULI (eds)
285 Rational Points on Curves over Finite Fields: Theory and Applications, H. NIEDERREITER & C. XING
286 Clifford Algebras and spinors 2ed, P. LOUNESTO
287 Topics on Riemann surfaces and Fuchsian groups, E. BUJALANCE, A. F. COSTA & E. MARTINEZ (eds)
288 Surveys in Combinatorics, 2001, J. W. P. Hirschfeld (ed)

London Mathematical Society Lecture Note Series. 288

Rational Points on Curves over Finite Fields: Theory and Applications

Harald Niederreiter
National University of Singapore

Chaoping Xing
National University of Singapore

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011–4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2001
Reprinted 2002

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this book is available from the British Library

ISBN 0 521 66543 4 paperback

To Gerlinde and Youqun Shi

Contents

Preface

Algebraic curves over finite fields and their function fields have been and are still a source of great fascination for number theorists and geometers alike, ever since the seminal work of Hasse and Weil in the 1930s and 1940s. Many important and fruitful ideas have arisen out of this area, where number theory and algebraic geometry meet, and these developments have even spawned a new subject called arithmetic algebraic geometry which now has a broad appeal.

For a long time, the study of algebraic curves over finite fields and their function fields was the province of pure mathematicians. But then, in a series of three papers in the period 1977–1982, Goppa found stunning applications of algebraic curves over finite fields, and especially of those with many rational points, to coding theory. This created a much stronger interest in the area and attracted new groups of researchers such as coding theorists and algorithmically inclined mathematicians. An added incentive was provided by the invention of elliptic-curve cryptosystems in 1985. Algebraic geometry over finite fields is a flourishing subject nowadays which produces exciting research and is immensely relevant for applications.

There has been tremendous research activity focused on algebraic curves over finite fields and their function fields in the last five years. Important theoretical advances were achieved, such as new techniques of constructing algebraic curves over finite fields with many rational points, or equivalently global function fields with many rational places, and improved lower bounds on $A(q)$, the crucial quantity in the asymptotic theory of the number of $\mathbf{F}_q$-rational points on algebraic curves over the finite field $\mathbf{F}_q$ of order q. Explicit towers of global function fields meeting the Vlăduţ-Drinfeld bound were constructed for the first time. These and other results have a significant impact on coding theory since they lead, in particular, to sequences of algebraic-geometry codes of increasing length that beat the asymptotic Gilbert-Varshamov bound, the classical benchmark for families of good linear codes. Algebraic-geometry codes have received a further impetus from completely new methods of constructing linear codes from algebraic curves over finite fields that allow a much greater flexibility than Goppa's construction. It is equally important that entirely new areas of applications have opened up for algebraic curves over finite fields and their function fields in the last five years. These include stream ciphers, hash functions, and authentication schemes in cryptography as well as the construction of low-discrepancy sequences for quasi-Monte Carlo methods. In all these applications, the methods of algebraic geometry have been more successful than classical approaches.

The main aim of this book is to make interested graduate students and researchers conversant with these recent developments, by not only offering a unified exposition of the relevant results and techniques, but also providing the necessary background as far as possible in a limited space. An ideal preparation for reading this book will be the study of Stichtenoth's excellent monograph *Algebraic Function Fields and Codes*. A prior exposure to class field theory will also be helpful for the reader. Summaries of pertinent facts on algebraic function fields and class field theory can be found in Chapters 1 and 2 of the present book, together with appropriate references.

Just like Stichtenoth's book and most of the recent research papers on the topics of relevance here, our book favors the function-field viewpoint over the algebraic-geometry viewpoint. It is our experience that, particulary for students with a background in classical algebra and number theory, the language of global function fields is easier to master than that of projective curves over finite fields, mainly because of the close analogy between global function fields and algebraic number fields. The two viewpoints are, of course, equivalent, and a succinct discussion of the algebraic-geometry viewpoint, and in particular of the connections between global function fields and smooth projective curves over finite fields, is presented in Appendix A of this book.

As mentioned above, Chapter 1 on algebraic function fields and Chapter 2 on the class field theory of global function fields are of an introductory character. Chapter 3 surveys explicit global function fields that are useful for the following core chapter, in which recent work on the construction of global function fields with many rational places is discussed. In Chapter 4 we have emphasized methods that lead to general results and are not just *ad hoc* techniques. Another core part is Chapter 5 which studies the asymptotic behavior of the number of rational places of global function fields when the genus tends to infinity, again with a focus on recent research. The remaining three chapters are devoted to applications. Chapter 6 discusses the well-known use of algebraic-geometry methods in coding theory, but we go beyond the several textbooks on this subject by also covering results of the last few years. Chapters 7 and 8 present the recent applications to cryptography, respectively low-discrepancy sequences, that we mentioned earlier in this preface. In all three applications-oriented chapters we include some background on the underlying target area for a better appreciation of the material.

We express our gratitude to the Austrian Academy of Sciences and the National University of Singapore for sponsoring mutual visits of the authors in crucial periods of this book project. We are grateful also to Helmut Kopka for having given to the world the treasure trove of a book *LaTeX: Einführung* which proved invaluable in all TEXnical matters. It is a pleasure to thank the staff of Cambridge University Press, and in particular Roger Astley, for being so receptive to our idea of writing this book and for seeing through, and advising on, the project with their usual professionalism.

Singapore, October 2000

HARALD NIEDERREITER
CHAOPING XING