

**A Selection of Books, Papers, and Theses  
Citing Magma**

Computational Algebra Group  
University of Sydney

January 17, 2024

# Contents

<b>Overview of the Bibliography</b>	<b>1</b>
Introduction . . . . .	1
Citing MAGMA in Publications . . . . .	1
Bibliography Files . . . . .	2
Acknowledgements . . . . .	2

## Mathematics

<b>Algebraic Geometry</b>	<b>4</b>
Foundations . . . . .	4
Local Theory . . . . .	5
Cycles and Subschemes . . . . .	6
Families and Fibrations . . . . .	7
Birational Geometry . . . . .	8
Homology and Cohomology Theory . . . . .	9
Arithmetic and Diophantine Geometry . . . . .	10
Curves . . . . .	16
Surfaces and Higher Dimensional Varieties . . . . .	21
Abelian Varieties and Schemes . . . . .	27
Algebraic Groups . . . . .	28
Special Varieties . . . . .	30
Real Algebraic Geometry . . . . .	32
Computational Methods . . . . .	33
<b>Algebraic Structures</b>	<b>36</b>
Ordered Structures . . . . .	36
<b>Algebras – Associative</b>	<b>37</b>
Associative Algebras: General . . . . .	37
Modules and Ideals . . . . .	38
Representation Theory . . . . .	39
Orders and Arithmetic . . . . .	40
Division Rings and Semisimple Artin Rings . . . . .	41
Algebras from Standard Constructions . . . . .	42
Computational Methods . . . . .	44

<b>Algebras – Non-Associative</b>	<b>46</b>
Nonassociative Algebras: General . . . . .	46
Lie Algebras . . . . .	47
Quantum Groups . . . . .	50
Computational Methods . . . . .	51
<b>Analysis</b>	<b>52</b>
Analysis: General . . . . .	52
Riemann Surfaces . . . . .	53
Functions of Several Complex Variables . . . . .	55
Ordinary Differential Equations . . . . .	56
Partial Differential Equations . . . . .	59
Dynamical Systems . . . . .	60
Operator Algebras . . . . .	62
<b>Category Theory</b>	<b>63</b>
All Areas . . . . .	63
<b>Combinatorics</b>	<b>64</b>
Enumerative Combinatorics . . . . .	64
Designs and Configurations . . . . .	65
Graph Theory . . . . .	73
Extremal Combinatorics . . . . .	85
Algebraic Combinatorics . . . . .	86
Computational Methods . . . . .	89
<b>Commutative Algebra</b>	<b>91</b>
Commutative Algebra: General . . . . .	91
Invariant Theory . . . . .	92
Modules and Ideals . . . . .	97
Homological Methods . . . . .	98
Differential Algebra . . . . .	100
Computational Methods . . . . .	102
<b>Field Theory</b>	<b>111</b>
Field Theory: General . . . . .	111
Extensions and Galois Theory . . . . .	112

Semifields and Near-fields . . . . .	115
Computational Methods . . . . .	116
<b>Geometry</b>	<b>118</b>
Incidence Geometry . . . . .	118
Finite Geometry . . . . .	120
Real and Complex Geometry . . . . .	134
General Convexity . . . . .	135
Polytopes and Polyhedra . . . . .	136
Discrete Geometry . . . . .	138
Differential Geometry . . . . .	140
<b>Group Theory</b>	<b>141</b>
Permutation Groups . . . . .	141
Representation Theory . . . . .	146
Abstract Finite Groups . . . . .	159
Structure and Classification . . . . .	174
Special Aspects of Finite or Infinite Groups . . . . .	176
Linear Algebraic Groups . . . . .	186
Matrix Groups (not Linear Algebraic) . . . . .	192
Cohomology . . . . .	194
Loops, Quasigroups and Semigroups . . . . .	197
Computational Group Theory . . . . .	198
<b><i>K</i>-Theory</b>	<b>213</b>
All Areas . . . . .	213
<b>Linear Algebra</b>	<b>214</b>
Linear Algebra and Matrices . . . . .	214
Computational Linear Algebra . . . . .	215
<b>Mathematical Education</b>	<b>218</b>
Computer-Assisted Learning . . . . .	218
<b>Number Theory</b>	<b>219</b>
Elementary Number Theory . . . . .	219
Primality and Factorisation . . . . .	220

Sequences and Sets . . . . .	221
Diophantine Equations . . . . .	223
Forms and Linear Algebraic Groups . . . . .	230
Discontinuous Groups and Automorphic Forms . . . . .	232
Arithmetic Algebraic Geometry . . . . .	241
Geometry of Numbers . . . . .	261
Probabilistic Theory . . . . .	265
Zeta and $L$ -functions: Analytic Theory . . . . .	266
Additive and Multiplicative Number Theory . . . . .	268
Algebraic Number Theory . . . . .	269
Finite Fields . . . . .	277
Computational Methods . . . . .	280
<b>Numerical Analysis</b>	<b>292</b>
All Areas . . . . .	292
<b>Probability and Statistics</b>	<b>293</b>
Probability . . . . .	293
Statistics . . . . .	295
<b>Topological and Lie Groups</b>	<b>296</b>
Lie Groups . . . . .	296
Noncompact Transformation Groups . . . . .	297
<b>Topology</b>	<b>298</b>
General Topology . . . . .	298
Algebraic Topology . . . . .	299
Homology Theory . . . . .	301
Spectral Sequences . . . . .	303
Low-dimensional Topology . . . . .	304
Topological Manifolds . . . . .	308
Topological Groups . . . . .	309
Computational Topology . . . . .	310

**Information, Communication, and Computation**

<b>Coding Theory</b>	<b>311</b>
Linear Codes: General . . . . .	311
Cyclic Codes . . . . .	317
Self-Dual Codes . . . . .	321
Algebraic Geometry Codes . . . . .	328
Combinatorial Codes . . . . .	331
Codes over Galois Rings . . . . .	337
Low-Density Parity Check Codes . . . . .	339
Lattice Codes . . . . .	341
Quantum Error-Correcting Codes . . . . .	342
Computational Methods . . . . .	345
<b>Computer Science</b>	<b>346</b>
Computer System Organization . . . . .	346
Software . . . . .	347
Theory of Computing . . . . .	350
Artificial Intelligence . . . . .	352
Computing Methodologies . . . . .	355
Symbolic and Computational Algebra . . . . .	356
<b>Cryptography</b>	<b>358</b>
Cryptography: General . . . . .	358
Block Ciphers . . . . .	361
Stream Ciphers . . . . .	363
Public Key Cryptography . . . . .	365
Curve-Based Cryptography . . . . .	372
Protocols . . . . .	380
Random Number Generators . . . . .	381
Computational Methods . . . . .	382
<b>Information and Communication</b>	<b>385</b>
Information . . . . .	385
Circuits and Networks . . . . .	386
Signal Processing . . . . .	387
Data Mining . . . . .	388

**Physical and Social Sciences**

<b>Biology</b>	<b>389</b>
Mathematical Biology . . . . .	389
<b>Chemistry</b>	<b>390</b>
Chemistry . . . . .	390
<b>Economics</b>	<b>392</b>
Mathematical Economics . . . . .	392
<b>Operations Research</b>	<b>393</b>
Operations Research . . . . .	393
Mathematical Programming . . . . .	394
<b>Physics</b>	<b>395</b>
Mechanics . . . . .	395
Quantum Theory . . . . .	396
Quantum Computation . . . . .	397
Statistical Mechanics . . . . .	400
Relativity and Gravitation . . . . .	401
Geophysics . . . . .	402

# Overview of the Bibliography

## Introduction

For the successful evolution of MAGMA it is important that we have a detailed knowledge as to where and how it is applied. As one approach to obtaining such information we have undertaken a fairly unsophisticated sweep of the web for publications that refer to MAGMA or Cayley (the predecessor of MAGMA), either in the bibliography or in the text proper.

Approximately 3000 publications have been found; of these, approximately 200 refer to Cayley and around 2800 refer to MAGMA. In the list published below we have included books, papers, PhD theses, preprints in the `arXiv` (unless they are published), and a small number of preprints that are of special interest. Some 200 items referring to MAGMA have been omitted. These comprise:

- (i) Published papers where the reference to MAGMA was minor or incidental to the research;
- (ii) Most unpublished papers unless they are stored in the `arXiv`.

This culling procedure is not complete as there are many items where we have lacked either time or access to the text. So the reader should be aware that the current version includes a few items which will be eventually removed on the basis of limited relevance to the aims of this exercise.

One feature of the database is the classification of the items into categories based substantially on MSC codes. This helps identify those areas of mathematics in which MAGMA finds a significant number of applications. We hope that users working in a given area may find it useful to be able to see how others have applied MAGMA to problems in that area. We plan at a future time to do a more detailed analysis on a selection of the papers in order to gain a deeper understanding of the role MAGMA plays.

Details on these publications are available below. We welcome corrections and additions to this list—if you have an appropriate publication not included in the current list, please email us with the publication details.

## Citing Magma in Publications

As the funding for MAGMA is provided by competitive research grants, it is important for us to be able to present evidence of the impact of the system by providing evidence of citations in the literature. If you use MAGMA in a non-trivial way in your research then



we strongly encourage you to mention this in the text and also to include a citation in the bibliography. If your paper does not include some standard reference for MAGMA in its bibliography then it is much harder for us to locate it on the web since it will not show up in citation indexes.

The recommended citation is:

W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput. (3–4) **24** (1997), 235–265.

Alternatively, you could cite the MAGMA Handbook:

W. Bosma, J. Cannon, C. Fieker, and A. Steel (Eds.) *Handbook of Magma Functions*, Edition 2.16 (2010), 5017 pages.

If using this second form, you should replace the last portion with the appropriate details for the version of the Handbook that corresponds to the version of MAGMA used in your application.

## Bibliography Files

The bibliography is available in two forms:

- (i) A list of papers which cite MAGMA, culled as described earlier and sorted (roughly) using a modified version of the MSC 2010 codes;
- (ii) A list of papers which cite either MAGMA or Cayley, presented in alphabetical order by first author.

These lists, together with lists covering individual areas and topics, are available as PDF files from the MAGMA website:

<http://magma.maths.usyd.edu.au/magma/citations/>

Please check to see whether all of your papers have been recorded.

## Acknowledgements

An initial search by Michael Gleeson in early 2006 located approximately 1000 papers. In early 2007, Paul Tiffen identified a further 900 papers and this was the basis of the 2007 edition of this bibliography. Paul Tiffen collected a further 700 papers in 2008 and early

2009 while Michael Gleeson added a further 400 papers in September 2009. A pruned version of these lists formed the basis of the 2009 edition.

The papers on coding theory up to 2006 were collected by Greg White. Amongst others, Philippe Cara, Marston Conder, Markus Grassl, Masaaki Harada, George Havas, Jenny Key, Dimitri Leemans, Eamonn O'Brien, and Martin Rötteler were kind enough to provide us with lists of their publications relating to Cayley and MAGMA.

We acknowledge the debt we owe to the Mathematical Reviews database which greatly facilitated this exercise.

# Algebraic Geometry

## Foundations

14Axx

- [1] E. Ballico, E. Gasparim, and T. Kölppe, *Vector bundles near negative curves: Moduli and local Euler characteristic*, *Comm. Algebra* **37** (2009), no. 8, 2688–2713.
- [2] Pavel Etingof and Victor Ginzburg, *Noncommutative complete intersections and matrix integrals*, *Pure Appl. Math. Q.* **3** (2007), no. 1, part 3, 107–151. MR MR2330156 (2008b:16044)

# Local Theory

14Bxx

- [1] Stefan Schröer, *Singularities appearing on generic fibers of morphisms between smooth schemes*, Michigan Math. J. **56** (2008), no. 1, 55–76. MR MR2433656 (2009i:14003)

# Cycles and Subschemes

14Cxx

- [1] Timothy G. Abbott, Kiran S. Kedlaya, and David Roe, *Bounding Picard numbers of surfaces using  $p$ -adic cohomology*, 2006.
- [2] Anita Buckley and Balázs Szendrői, *Orbifold Riemann-Roch for threefolds with an application to Calabi-Yau geometry*, J. Algebraic Geom. **14** (2005), no. 4, 601–622. MR MR2147356 (2006b:14013)
- [3] Ulrich Derenthal, *On the Cox ring of del Pezzo surfaces*, 2006.
- [4] Pierre Guillot, *The Chow rings of  $G_2$  and  $Spin(7)$* , J. Reine Angew. Math. **604** (2007), 137–158. MR MR2320315
- [5] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR MR1890579 (2003j:14032)
- [6] David Joyner and Amy Ksir, *Modular representations on some Riemann-Roch spaces of modular curves  $X(N)$* , Computational Aspects of Algebraic Curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 163–205. MR MR2182040 (2006k:11112)
- [7] Roger Oyono, *Non-hyperelliptic modular Jacobians of dimension 3*, Math. Comp. **78** (2009), no. 266, 1173–1191. MR MR2476578
- [8] Magda Sebestean, *Correspondance de McKay et Equivalences Derivees*, Ph.D. thesis, Paris VII, 2005, p. 169.
- [9] Kaori Suzuki, *On Fano indices of  $Q$ -Fano 3-folds*, Manuscripta Math. **114** (2004), no. 2, 229–246. MR MR2067795 (2005c:14046)
- [10] Ronald van Luijk,  *$K3$  surfaces with Picard number one and infinitely many rational points*, Algebra and Number Theory **1** (2007), no. 1, 1–15.

# Families and Fibrations

14Dxx

- [1] Anthony Henderson and Eric Rains, *The cohomology of real De Concini-Procesi models of Coxeter type*, Int. Math. Res. Not. IMRN (2008), no. 7, Art. ID rnn001, 29. MR MR2428302
- [2] Benjamin Howard, John Millson, Andrew Snowden, and Ravi Vakil, *The equations for the moduli space of  $n$  points on the line*, Duke Math. J. **146** (2009), no. 2, 175–226. MR MR2477759 (2009m:14070)
- [3] Alan G.B. Lauder, *Degenerations and limit Frobenius structures in rigid cohomology*, 2009.
- [4] Claus Lehr and Michel Matignon, *Wild monodromy and automorphisms of curves*, Duke Math. J. **135** (2006), no. 3, 569–586. MR MR2272976 (2008a:14039)
- [5] Adrien Poteaux, *Computing monodromy groups defined by plane algebraic curves*, SNC'07, ACM, New York, 2007, pp. 36–45. MR MR2404912
- [6] Carlos Rito, *On surfaces with  $p_g = q = 1$  and non-ruled bicanonical involution*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **6** (2007), no. 1, 81–102. MR MR2341516
- [7] Kira Samol and Duco van Straten, *Frobenius polynomials for Calabi-Yau equations*, Commun. Number Theory Phys. **2** (2008), no. 3, 537–561. MR MR2482942
- [8] James P Smith, *Picard-Fuchs differential equations for families of K3 surfaces*, Ph D thesis, University of Warwick, 2007.
- [9] H. A. Verrill, *Sums of squares of binomial coefficients, with applications to Picard-Fuchs equations*, 2004.
- [10] Bianca Viray, *A family of varieties with exactly one pointless rational fiber*, 2009.

# Birational Geometry

14Exx

- [1] I. C. Bauer, F. Catanese, and F. Grunewald, *The classification of surfaces with  $p_g = q = 0$  isogenous to a product of curves*, Pure Appl. Math. Q. **4** (2008), no. 2, part 1, 547–586. MR MR2400886 (2009a:14046)
- [2] Christian Böhning, *The rationality of the moduli space of curves of genus 3 after P. Katsylo*, 2008.
- [3] Gavin Brown and Daniel Ryder, *Elliptic fibrations on cubic surfaces*, J. Pure Appl. Algebra **214** (2010), no. 4, 410–421. MR MR2558749
- [4] Laurent Busé and Jean-Pierre Jouanolou, *On the closed image of a rational map and the implicitization problem*, J. Algebra **265** (2003), no. 1, 312–357. MR MR1984914 (2004e:14024)
- [5] Tetsuo Nakano, *On the moduli space of pointed algebraic curves of low genus. II. Rationality*, Tokyo J. Math. **31** (2008), no. 1, 147–160. MR MR2426799
- [6] Tetsuo Nakano and Hiroyasu Nishikubo, *On some maximal Galois coverings over affine and projective planes. II*, Tokyo J. Math. **23** (2000), no. 2, 295–310. MR MR1806466 (2002a:14014)
- [7] Stavros Argyrios Papadakis, *Type II unprojection*, J. Algebraic Geom. **15** (2006), no. 3, 399–414. MR MR2219843
- [8] Miles Reid, *Graded rings and birational geometry*, 2000.

# Homology and Cohomology Theory

14Fxx

- [1] Timothy G. Abbott, Kiran S. Kedlaya, and David Roe, *Bounding Picard numbers of surfaces using  $p$ -adic cohomology*, 2006.
- [2] Martin Bright, *Brauer groups of diagonal quartic surfaces*, J. Symbolic Comput. **41** (2006), no. 5, 544–558. MR MR2209163
- [3] Michael Dettweiler and Stefan Reiter, *On exceptional rigid local systems*, 2006.
- [4] Anthony Henderson and Eric Rains, *The cohomology of real De Concini-Procesi models of Coxeter type*, Int. Math. Res. Not. IMRN (2008), no. 7, Art. ID rnn001, 29. MR MR2428302
- [5] Kiran S. Kedlaya, *Computing zeta functions via  $p$ -adic cohomology*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 1–17. MR MR2137340 (2006a:14033)
- [6] Andrew Kresch and Yuri Tschinkel, *On the arithmetic of del Pezzo surfaces of degree 2*, Proc. London Math. Soc. (3) **89** (2004), no. 3, 545–569. MR MR2107007 (2005h:14060)
- [7] ———, *Effectivity of Brauer-Manin obstructions*, Adv. Math. **218** (2008), no. 1, 1–27. MR MR2409407
- [8] G. I. Lehrer, *The cohomology of the regular semisimple variety*, J. Algebra **199** (1998), no. 2, 666–689. MR MR1489931 (98k:20080)
- [9] Stefan Schröer, *Singularities appearing on generic fibers of morphisms between smooth schemes*, Michigan Math. J. **56** (2008), no. 1, 55–76. MR MR2433656 (2009i:14003)



# Arithmetic and Diophantine Geometry

14Gxx

- [1] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR MR2183527
- [2] Edoardo Ballico, Antonio Cossidente, and Alessandro Siciliano, *External flats to varieties in symmetric product spaces over finite fields*, Finite Fields Appl. **9** (2003), no. 3, 300–309. MR MR1983050 (2004c:14041)
- [3] Tatiana Bandman, Gert-Martin Greuel, Fritz Grunewald, Boris Kunyavskii, Gerhard Pfister, and Eugene Plotkin, *Identities for finite solvable groups and equations in finite simple groups*, Compos. Math. **142** (2006), no. 3, 734–764. MR MR2231200 (2007d:20027)
- [4] Arthur Baragar and Ronald van Luijk, *K3 surfaces with Picard number three and canonical vector heights*, Math. Comp. **76** (2007), no. 259, 1493–1498 (electronic). MR MR2299785
- [5] M. Borovoi, J.-L. Colliot-Thélène, and A. N. Skorobogatov, *The elementary obstruction and homogeneous spaces*, Duke Math. J. **141** (2008), no. 2, 321–364. MR MR2376817
- [6] Nigel Boston, *Reducing the Fontaine-Mazur conjecture to group theory*, Progress in Galois theory, Dev. Math., vol. 12, Springer, New York, 2005, pp. 39–50. MR MR2148459
- [7] Kristian Brander, *An optimal unramified tower of function fields*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 351–365. MR MR2484064 (2010b:14051)
- [8] Friederike Brezing and Annegret Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. **37** (2005), no. 1, 133–141. MR MR2165045
- [9] Ezra Brown, Bruce T. Myers, and Jerome A. Solinas, *Hyperelliptic curves with compact parameters*, Des. Codes Cryptogr. **36** (2005), no. 3, 245–261. MR MR2162578

- [10] Nils Bruin, *Visualising  $\text{Sha}[2]$  in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic). MR MR2047096 (2005c:11067)
- [11] Jan H. Bruinier and Tonghai Yang, *CM values of automorphic Green functions on orthogonal groups over totally real fields*, 2010.
- [12] Patrick Corn, *The Brauer-Manin obstruction on del Pezzo surfaces of degree 2*, Proc. Lond. Math. Soc. (3) **95** (2007), no. 3, 735–777. MR MR2368282 (2009a:14027)
- [13] Patrick Corn, *Tate-Shafarevich groups and K3 surfaces*, Math. Comp. **To appear** (2007).
- [14] R. de la Bret'che and T.D. Browning, *Manin's conjecture for quartic del Pezzo surfaces with a conic fibration*, 2008.
- [15] Jan Denef and Frederik Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 308–323. MR MR2041093 (2005d:11088)
- [16] Xander Faber and Benjamin Hutz, *On the number of rational iterated pre-images of the origin under quadratic dynamical systems*, 2008.
- [17] Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve, *Uniform bounds on pre-images under quadratic dynamical systems*, Math. Res. Lett. **16** (2009), no. 1, 87–101. MR MR2480563
- [18] Tom Fisher, *A new approach to minimising binary quartics and ternary cubics*, Math. Res. Lett. **14** (2007), no. 4, 597–613. MR MR2335986 (2008k:11058)
- [19] ———, *Finding rational points on elliptic curves using 6-descent and 12-descent*, J. Algebra **320** (2008), no. 2, 853–884. MR MR2422319
- [20] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. MR MR2103661 (2005j:11047)
- [21] David Freeman and Kristin Lauter, *Computing endomorphism rings of Jacobians of genus 2 curves over finite fields*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 29–66. MR MR2484047

- [22] Steven D. Galbraith, *Weil descent of Jacobians*, Discrete Appl. Math. **128** (2003), no. 1, 165–180, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991424 (2004m:14046)
- [23] Steven D. Galbraith and Xibin Lin, *Computing pairings using  $x$ -coordinates only*, Des. Codes Cryptogr. **50** (2009), no. 3, 305–324. MR MR2480678
- [24] Ralf Gerkmann, *Relative rigid cohomology and deformation of hypersurfaces*, Int. Math. Res. Pap. IMRP (2007), no. 1, Art. ID rpm003, 67. MR MR2334009
- [25] Josep González and Victor Rotger, *Non-elliptic Shimura curves of genus one*, J. Math. Soc. Japan **58** (2006), no. 4, 927–948. MR MR2276174 (2007k:11093)
- [26] Cem Güneri, Henning Stichtenoth, and Ihsan Taşkın, *Further improvements on the designed minimum distance of algebraic geometry codes*, J. Pure Appl. Algebra **213** (2009), no. 1, 87–97. MR MR2462987
- [27] Johan P. Hansen, *Toric varieties, Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 4, 289–300. MR MR1953195 (2003j:14029)
- [28] David Harari and Tamás Szamuely, *Galois sections for abelianized fundamental groups*, Math. Ann. **344** (2009), no. 4, 779–800, With an appendix by E. V. Flynn. MR MR2507624
- [29] Florian Hess, *A note on the Tate pairing of curves over finite fields*, Arch. Math. (Basel) **82** (2004), no. 1, 28–32. MR MR2034467 (2004m:14040)
- [30] Christopher Holden, *Mod 4 Galois representations and elliptic curves*, Proc. Amer. Math. Soc. **136** (2008), no. 1, 31–39 (electronic). MR MR2350385
- [31] David Holmes, *Canonical heights on hyperelliptic curves and effective  $Q$ -factoriality for arithmetic surfaces*, 2010. MR 14G40; 11G30, 11G50, 37P30
- [32] E. W. Howe and K. E. Lauter, *Improved upper bounds for the number of points on curves over finite fields*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 6, 1677–1737. MR MR2038778 (2005c:11079)
- [33] Everett W. Howe, *Supersingular genus-2 curves over fields of characteristic 3*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 49–69. MR MR2459989 (2009j:11103)

- [34] Everett W. Howe, Kristin E. Lauter, and Jaap Top, *Pointless curves of genus three and four*, Arithmetic, Geometry and Coding Theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 125–141. MR MR2182840 (2006g:11125)
- [35] Nathan Owen Ilten and Hendrik Süß, *AG codes from polyhedral divisors*, 2008.
- [36] Farzali A. Izadi and V. Kumar Murty, *Counting points on an abelian variety over a finite field*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 323–333. MR MR2092391 (2005f:11127)
- [37] Rafe Jones and Jeremy Rouse, *Iterated endomorphisms of abelian algebraic groups*, Proc. London Math. Soc. **100** (2010), 763–794.
- [38] Samuel Kadziela, *Rigid analytic uniformization of curves and the study of isogenies*, Acta Appl. Math. **99** (2007), no. 2, 185–204. MR MR2350208
- [39] Kiran S. Kedlaya, *Computing zeta functions via  $p$ -adic cohomology*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 1–17. MR MR2137340 (2006a:14033)
- [40] Kenji Koike and Annegret Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518 (electronic). MR MR2085904 (2005g:11103)
- [41] Aristides Kontogeorgis and Victor Rotger, *On abelian automorphism groups of Mumford curves and applications to Shimura curves*, 2006.
- [42] Andrew Kresch and Yuri Tschinkel, *Integral points on punctured abelian surfaces*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 198–204. MR MR2041084 (2005d:11081)
- [43] ———, *On the arithmetic of del Pezzo surfaces of degree 2*, Proc. London Math. Soc. (3) **89** (2004), no. 3, 545–569. MR MR2107007 (2005h:14060)
- [44] ———, *Effectivity of Brauer-Manin obstructions*, Adv. Math. **218** (2008), no. 1, 1–27. MR MR2409407
- [45] L. Kulesz, G. Matera, and É. Schost, *Uniform bounds on the number of rational points of a family of curves of genus 2*, J. Number Theory **108** (2004), no. 2, 241–267. MR MR2098638 (2005h:11130)

- [46] Gilles Lachaud and Christophe Ritzenthaler, *On a conjecture of Serre on abelian threefolds*, Algebraic Geometry and its applications, Proceedings of the First SAGA conference, Papeete, France 2007, 2008, pp. 1–28.
- [47] Alan G. B. Lauder, *Counting solutions to equations in many variables over finite fields*, Found. Comput. Math. **4** (2004), no. 3, 221–267. MR MR2078663 (2005f:14048)
- [48] ———, *A recursive method for computing zeta functions of varieties*, LMS J. Comput. Math. **9** (2006), 222–269 (electronic). MR MR2261044 (2007g:14022)
- [49] F. Leprévost, M. Pohst, and A. Schöpp, *Rational torsion of  $J_0(N)$  for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10*, Abh. Math. Sem. Univ. Hamburg **74** (2004), 193–203. MR MR2112831 (2005h:11131)
- [50] John Little and Hal Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), no. 4, 999–1014 (electronic). MR MR2272243
- [51] Adam Logan, *The Brauer-Manin obstruction on del Pezzo surfaces of degree 2 branched along a plane section of a Kummer surface*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 3, 603–622. MR MR2418706
- [52] Michelle Manes,  *$Q$ -rational cycles for degree-2 rational maps having an automorphism*, Proc. Lond. Math. Soc. (3) **96** (2008), no. 3, 669–696. MR MR2407816 (2009a:14029)
- [53] David Savitt, *The maximum number of points on a curve of genus 4 over  $F_8$  is 25*, Canad. J. Math. **55** (2003), no. 2, 331–352, With an appendix by Kristin Lauter. MR MR1969795 (2004i:11059)
- [54] Éric Schost, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 5, 349–393. MR MR1959170 (2003k:13035)
- [55] R. Shaw, *The polynomial degrees of Grassmann and Segre varieties over  $GF(2)$* , Discrete Math. **308** (2008), no. 5-6, 872–879. MR MR2378937
- [56] Edlyn Teske, *An elliptic curve trapdoor system (extended abstract)*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 341–352. MR MR2076258

- [57] Ronald van Luijk, *Quartic K3 surfaces without nontrivial automorphisms*, Math. Res. Lett. **13** (2006), no. 2-3, 423–439. MR MR2231128 (2007b:14084)
- [58] Ronald van Luijk, *Cubic points on cubic curves and the Brauer-Manin obstruction on K3 surfaces*, 2007.
- [59] Bianca Viray, *A family of varieties with exactly one pointless rational fiber*, 2009.
- [60] John Voight, *Shimura curves of genus at most two*, Math. Comp. **78** (2009), no. 266, 1155–1172. MR MR2476577
- [61] Gabor Wiese, *Dihedral Galois representations and Katz modular forms*, Doc. Math. **9** (2004), 123–133 (electronic). MR MR2054983 (2005c:11065)

# Curves

14Hxx

- [1] S. Arita, S. Miura, and T. Sekiguchi, *An addition algorithm on the Jacobian varieties of curves*, J. Ramanujan Math. Soc. **19** (2004), no. 4, 235–251. MR MR2125500 (2005m:14114)
- [2] Philip Boalch, *Higher genus icosahedral Painlevé curves*, Funk. Ekvac. (Kobe), **50** (2007), 19–32.
- [3] Irene I. Bouw and Stefan Wewers, *Indigenous bundles with nilpotent  $p$ -curvature*, Int. Math. Res. Not. (2006), Art. ID 89254, 37. MR MR2219211
- [4] Louis Hugo Brewis, *Liftable  $D_4$ -covers*, Manuscripta Math. **126** (2008), no. 3, 293–313. MR MR2411230
- [5] Nils Bruin, *The arithmetic of Prym varieties in genus 3*, Compos. Math. **144** (2008), no. 2, 317–338. MR MR2406115
- [6] Nils Bruin and Kevin Doerksen, *The arithmetic of genus two curves with  $(4,4)$ -split Jacobians*, arXiv:0902.3480v2 (2010).
- [7] E. Bujalance, Marston Conder, J. M. Gamboa, G. Gromadzki, and M. Izquierdo, *Double coverings of Klein surfaces by a given Riemann surface*, J. Pure Appl. Algebra **169** (2002), no. 2-3, 137–151. MR MR1897339 (2003e:14023)
- [8] Emilio Bujalance, F. J. Cirre, and Marston Conder, *On extendability of group actions on compact Riemann surfaces*, Trans. Amer. Math. Soc. **355** (2003), no. 4, 1537–1557 (electronic). MR MR1946404 (2003k:20079)
- [9] Gabriel Cardona, *Representations of  $G_k$ -groups and twists of the genus two curve  $y^2 = x^5 - x$* , J. Algebra **303** (2006), no. 2, 707–721. MR MR2255131 (2007e:14049)
- [10] Wouter Castryck and John Voight, *Nondegenerate curves of low genus over small finite fields*, Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 521, AMS, Providence, R.I., 2009, pp. 21–28.
- [11] J.-M. Couveignes, *Linearizing torsion classes in the Picard group of algebraic curves over finite fields*, J. Algebra **321** (2009), no. 8, 2085–2118. MR MR2501511

- [12] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, *Explicit  $n$ -descent on elliptic curves, II: Geometry*, J. reine angew. Math **2009** (2009), no. 632, 63–84.
- [13] Laurent Ducrohet, *The Frobenius action on rank 2 vector bundles over curves in small genus and small characteristic*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 4, 1641–1669. MR MR2566970
- [14] Tom Fisher, *Genus one curves defined by Pfaffians*, 2004.
- [15] ———, *Testing equivalence of ternary cubics*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 333–345. MR MR2282934 (2007j:11074)
- [16] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR MR2448246
- [17] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 1–28. MR MR2484046
- [18] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129. MR MR2444631 (2009j:94110)
- [19] P. Gaudry and É. Schost, *On the invariants of the quotients of the Jacobian of a curve of genus 2*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 373–386. MR MR1913484 (2003e:14020)
- [20] Martine Girard, *The group of Weierstrass points of a plane quartic with at least eight hyperflexes*, Math. Comp. **75** (2006), no. 255, 1561–1583 (electronic). MR MR2219046 (2007b:14072)
- [21] Martine Girard and David R. Kohel, *Classification of genus 3 curves in special strata of the moduli space*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 346–360. MR MR2282935
- [22] Edray Herber Goins and Davin Maddox, *Heron triangles via elliptic curves*, Rocky Mountain J. Math. **36** (2006), no. 5, 1511–1526. MR MR2285297



- [23] Enrique González-Jiménez and Roger Oyono, *Non-hyperelliptic modular curves of genus 3*, J. Number Theory **130** (2010), no. 4, 862–878. MR 2600407
- [24] Jordi Guàrdia, *Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 4, 1253–1283. MR MR2339331 (2008g:11105)
- [25] Robert Guralnick and John Shareshian, *Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points*, Mem. Amer. Math. Soc. **189** (2007), no. 886, vi+128, With an appendix by Guralnick and R. Stafford. MR MR2343794
- [26] Emmanuel Hallouin, *Study and computation of a Hurwitz space and totally real  $\mathrm{PSL}_2(F_8)$ -extensions of  $Q$* , J. Algebra **292** (2005), no. 1, 259–281. MR MR2166804 (2006h:14041)
- [27] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR MR1890579 (2003j:14032)
- [28] Florian Hess, *An algorithm for computing Weierstrass points*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 357–371. MR MR2041097 (2005b:14048)
- [29] Christopher Holden, *Mod 4 Galois representations and elliptic curves*, Proc. Amer. Math. Soc. **136** (2008), no. 1, 31–39 (electronic). MR MR2350385
- [30] Hendrik Hubrechts, *Quasi-quadratic elliptic curve point counting using rigid cohomology*, J. Symb. Comput. **44** (2009), no. 9, 1255–1267.
- [31] Samuel Kadziela, *Rigid analytic uniformization of curves and the study of isogenies*, Acta Appl. Math. **99** (2007), no. 2, 185–204. MR MR2350208
- [32] Sotiris Karanikolopoulos, *On holomorphic polydifferentials in positive characteristic*, 2010, p. 25.
- [33] A. Kontogeorgis, *The ramification sequence for a fixed point of an automorphism of a curve and the Weierstrass gap sequence*, Math. Z. **259** (2008), no. 3, 471–479. MR MR2395122 (2009a:14041)
- [34] Aristides Kontogeorgis and Victor Rotger, *On abelian automorphism groups of Mumford curves and applications to Shimura curves*, 2006.

- [35] Aristides Kontogeorgis and Yifan Yang, *Automorphisms of hyperelliptic modular curves  $X_0(n)$  in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144–163.
- [36] Aristides Kontogeorgis and Yifan Yang, *Automorphisms of hyperelliptic modular curves  $X_0(N)$  in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144–163. MR 2638986
- [37] D. Lehavi and C. Ritzenthaler, *An explicit formula for the arithmetic-geometric mean in genus 3*, Experiment. Math. **16** (2007), no. 4, 421–440. MR MR2378484 (2008k:14070)
- [38] Claus Lehr and Michel Matignon, *Wild monodromy and automorphisms of curves*, Duke Math. J. **135** (2006), no. 3, 569–586. MR MR2272976 (2008a:14039)
- [39] Adam Logan and Ronald van Luijk, *Nontrivial elements of Sha explained through K3 surfaces*, Math. Comp. **78** (2009), no. 265, 441–483. MR MR2448716
- [40] Kay Magaard, Tanush Shaska, and Helmut Völklein, *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Forum Math. **21** (2009), no. 3, 547–566. MR MR2526800
- [41] Coy L. May and Jay Zimmerman, *The groups of symmetric genus  $\sigma \leq 8$* , Comm. Algebra **36** (2008), no. 11, 4078–4095. MR MR2460404 (2009i:14038)
- [42] Josep M. Miret, Jordi Pujolàs, and Anna Rio, *Bisection for genus 2 curves in odd characteristic*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), no. 4, 55–60. MR MR2517297 (2010d:14039)
- [43] Santiago Molina, *Equations of hyperelliptic Shimura curves*, 2010.
- [44] Ian Morrison and David Swinarski, *Groebner techniques for low degree Hilbert stability*, 2009.
- [45] Tetsuo Nakano, *On the moduli space of pointed algebraic curves of low genus. II. Rationality*, Tokyo J. Math. **31** (2008), no. 1, 147–160. MR MR2426799
- [46] Laura Hitt O’Connor, Gary McGuire, Michael Naehrig, and Marco Streng, *CM construction of genus 2 curves with  $p$ -rank 1*, 2008.
- [47] Adrien Poteaux, *Computing monodromy groups defined by plane algebraic curves*, SNC’07, ACM, New York, 2007, pp. 36–45. MR MR2404912

- [48] Carlos Rito, *On the computation of singular plane curves and quartic surfaces*, 2010.
- [49] Magali Rocher, *Large  $p$ -group actions with a  $p$ -elementary abelian derived group*, Journal of Algebra **321** (2009), no. 2, 704 – 740.
- [50] Mohammad Sadek, *Counting models of genus one curves*, 2010.
- [51] Josef Schicho and David Sevilla, *Tschirnhaus-Weierstrass curves*, 2008.
- [52] Jasper Scholten and Hui June Zhu, *Families of supersingular curves in characteristic 2*, Math. Res. Lett. **9** (2002), no. 5-6, 639–650. MR MR1906067 (2003i:14038)
- [53] T. Shaska, *Computational aspects of hyperelliptic curves*, Computer Mathematics, Lecture Notes Ser. Comput., vol. 10, World Sci. Publishing, River Edge, NJ, 2003, pp. 248–257. MR MR2061839 (2005h:14073)
- [54] Tanush Shaska, *Determining the automorphism group of a hyperelliptic curve*, Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2003, pp. 248–254 (electronic). MR MR2035219 (2005c:14037)
- [55] Tony Shaska, *Genus 2 curves with  $(3, 3)$ -split Jacobian and large automorphism group*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 205–218. MR MR2041085 (2005e:14048)
- [56] Vijaykumar Singh and Gary McGuire, *The intersection of two Fermat hypersurfaces in  $P^3$  via computation of quotient curves*, 2009.
- [57] Paul B. van Wamelen, *Computing with the analytic Jacobian of a genus 2 curve*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 117–135. MR MR2278925
- [58] Yuri G. Zarhin, *Absolutely simple Prymians of trigonal curves*, Proceedings of the Steklov Institute of Mathematics **264** (2009), no. 1, 204–215.
- [59] Alexander Zvonkin, *Megamaps: Construction and examples*, Discrete Models: Combinatorics, Computation, and Geometry (Paris, 2001), Discrete Math. Theor. Comput. Sci. Proc., AA, Maison Inform. Math. Discrèt. (MIMD), Paris, 2001, pp. 329–339 (electronic). MR MR1888783 (2003d:14036)

# Surfaces and Higher Dimensional Varieties

14Jxx

- [1] Selma Altınok, Gavin Brown, and Miles Reid, *Fano 3-folds, K3 surfaces and graded rings*, Topology and Geometry: Commemorating SISTAG, Contemp. Math., vol. 314, Amer. Math. Soc., Providence, RI, 2002, pp. 25–53. MR MR1941620 (2004c:14077)
- [2] Arthur Baragar and Ronald van Luijk, *K3 surfaces with Picard number three and canonical vector heights*, Math. Comp. **76** (2007), no. 259, 1493–1498 (electronic). MR MR2299785
- [3] I. C. Bauer, F. Catanese, and F. Grunewald, *The classification of surfaces with  $p_g = q = 0$  isogenous to a product of curves*, Pure Appl. Math. Q. **4** (2008), no. 2, part 1, 547–586. MR MR2400886 (2009a:14046)
- [4] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald, *Beauville surfaces without real structures*, Geometric Methods in Algebra and Number Theory, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, pp. 1–42. MR MR2159375 (2006f:14040)
- [5] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald, *The absolute Galois group acts faithfully on the connected components of the moduli space of surfaces of general type*, 2007.
- [6] Ingrid Bauer, Fabrizio Catanese, Fritz Grunewald, and Roberto Pignatelli, *Quotients of a product of curves by a finite group and their fundamental groups*, 2008.
- [7] Ingrid Bauer, Fabrizio Catanese, and Roberto Pignatelli, *Surfaces of general type with geometric genus zero: A survey*, 2010.
- [8] Ingrid Bauer and Roberto Pignatelli, *The classification of minimal product-quotient surfaces with  $p_g = 0$* , 2010.
- [9] Ingrid C. Bauer and Fabrizio Catanese, *A volume maximizing canonical surface in 3-space*, Comment. Math. Helv. **83** (2008), no. 2, 387–406. MR MR2390050
- [10] Ingrid C. Bauer, Fabrizio Catanese, and Roberto Pignatelli, *Complex surfaces of general type: Some recent progress*, Global Aspects of Complex Geometry, Springer, Berlin, 2006, pp. 1–58. MR MR2264106

- [11] ———, *The moduli space of surfaces with  $K^2 = 6$  and  $p_g = 4$* , Math. Ann. **336** (2006), no. 2, 421–438. MR MR2244379
- [12] Tobias Beck, *Formal desingularization of surfaces: The Jung method revisited*, J. Symb. Comput. **44** (2009), no. 2, 131–160.
- [13] Tobias Beck and Josef Schicho, *Adjoint computation for hypersurfaces using formal desingularizations*, J. Algebra **320** (2008), no. 11, 3984–3996. MR MR2464803 (2009k:14029)
- [14] Gilberto Bini, *Quotients of hypersurfaces in weighted projective space*, 2009.
- [15] Martin Bright, *Brauer groups of diagonal quartic surfaces*, J. Symbolic Comput. **41** (2006), no. 5, 544–558. MR MR2209163
- [16] S. Allen Broughton, *Enumeration of the equisymmetric strata of the moduli space of surfaces of low genus*.
- [17] Gavin Brown, *Datagraphs in algebraic geometry and K3 surfaces*, Symbolic and Numerical Scientific Computation (Hagenberg, 2001), Lecture Notes in Comput. Sci., vol. 2630, Springer, Berlin, 2003, pp. 210–224. MR MR2043707 (2005a:14051)
- [18] ———, *Graded rings and special K3 surfaces*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 137–159. MR MR2278926
- [19] ———, *A database of polarized K3 surfaces*, Experiment. Math. **16** (2007), no. 1, 7–20. MR MR2312974
- [20] Gavin Brown, Alexander Kasprzyk, and Daniel Ryder, *Computational birational geometry of minimal rational surfaces*, 2009.
- [21] Gavin Brown and Kaori Suzuki, *Computing certain Fano 3-folds*, Japan J. Indust. Appl. Math. **24** (2007), no. 3, 241–250. MR MR2374989 (2008j:14076)
- [22] ———, *Fano 3-folds with divisible anticanonical class*, Manuscripta Math. **123** (2007), no. 1, 37–51. MR MR2300058 (2008a:14054)
- [23] Nils Bruin, *Visualising  $Sha[2]$  in abelian surfaces*, Math. Comp. **73** (2004), no. 247, 1459–1476 (electronic). MR MR2047096 (2005c:11067)

- [24] Anita Buckley and Balázs Szendrői, *Orbifold Riemann-Roch for threefolds with an application to Calabi-Yau geometry*, J. Algebraic Geom. **14** (2005), no. 4, 601–622. MR MR2147356 (2006b:14013)
- [25] Jorge Caravantes, *Low codimension Fano–Enriques threefolds*, 2006.
- [26] A. Clinger, C.F. Doran, J. Lewis, and U. Whitcher, *Normal forms, K3 surface moduli, and modular parametrizations*, Groups and Symmetries: Proceedings of the CRM conference in honor of John McKay,, CRM-AMS Proceedings and Lecture Notes, vol. 47, 2008.
- [27] Patrick Corn, *Tate-Shafarevich groups and K3 surfaces*, Math. Comp. **To appear** (2007).
- [28] Alessio Corti and Miles Reid, *Weighted Grassmannians*, Algebraic Geometry, de Gruyter, Berlin, 2002, pp. 141–163. MR MR1954062 (2003m:14076)
- [29] Willem A. de Graaf, Michael Harrison, Jana Pílníková, and Josef Schicho, *A Lie algebra method for rational parametrization of Severi-Brauer surfaces*, J. Algebra **303** (2006), no. 2, 514–529. MR MR2255120 (2007e:14058)
- [30] Willem A. de Graaf, Jana Pílníková, and Josef Schicho, *Parametrizing del Pezzo surfaces of degree 8 using Lie algebras*, J. Symbolic Comput. **44** (2009), no. 1, 1 – 14.
- [31] Ulrich Derenthal, *On the Cox ring of del Pezzo surfaces*, 2006.
- [32] Ulrich Derenthal, *Universal torsors of del Pezzo surfaces and homogeneous spaces*, Adv. Math. **213** (2007), no. 2, 849–864. MR MR2332612
- [33] Luis V. Dieulefait, *Computing the level of a modular rigid Calabi-Yau threefold*, Exp. Math **13** (2004), no. 2, 165–169.
- [34] Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007.
- [35] Pavel Etingof, Alexei Oblomkov, and Eric Rains, *Generalized double affine Hecke algebras of rank 1 and quantized del Pezzo surfaces*, Adv. Math. **212** (2007), no. 2, 749–796. MR MR2329319
- [36] Alice Garbagnati and Alessandra Sarti, *Elliptic fibrations and symplectic automorphisms on K3 surfaces*, Comm. Algebra **37** (2009), no. 10, 3601–3631. MR MR2561866

- [37] Shelly Garion and Matteo Penegini, *New Beauville surfaces, moduli spaces and finite groups*, 2009.
- [38] Victor Ginzburg, *Calabi-Yau algebras*, 2007.
- [39] Hans-Christian Graf v. Bothmer, *Finite field experiments*, Higher-dimensional Geometry over Finite Fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, pp. 1–62. MR MR2484075 (2009m:14032)
- [40] V. A. Gritsenko, K. Hulek, and G. K. Sankaran, *The Kodaira dimension of the moduli of K3 surfaces*, Invent. Math. **169** (2007), no. 3, 519–567. MR MR2336040
- [41] Johan P. Hansen, *Toric surfaces and codes, techniques and examples*, 2004.
- [42] Brendan Hassett, Anthony Vàrilly-Alvarado, and Patrick Varilly, *Transcendental obstructions to weak approximation on general K3 surfaces*, 2010.
- [43] Kiran S. Kedlaya, *Computing zeta functions of surfaces*, Mathematisches Forschungsinstitut Oberwolfach Report **32** (2005), 1808–1810.
- [44] Adam Logan, *The Brauer-Manin obstruction on del Pezzo surfaces of degree 2 branched along a plane section of a Kummer surface*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 3, 603–622. MR MR2418706
- [45] Stefan Maubach and Roel Willems, *Polynomial automorphisms over finite fields: Mimicking non-tame and tame maps by the Derksen group*, 2009.
- [46] Jan-Steffen Müller, *Explicit Kummer surface theory for arbitrary characteristic*, London Math. Soc. J. Comput. Math. **13** (2010), 47–64.
- [47] Francesco Polizzi, *Standard isotrivial fibrations with  $p_g = q = 1$* , Journal of Algebra **321** (2009), no. 6, 1600 – 1631.
- [48] Gopal Prasad and Sai-Kee Yeung, *Fake projective planes*, Invent. Math. **168** (2007), no. 2, 321–370. MR MR2289867
- [49] Carlos Rito, *On surfaces with  $p_g = q = 1$  and non-ruled bicanonical involution*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **6** (2007), no. 1, 81–102. MR MR2341516
- [50] ———, *A note on Todorov surfaces*, Osaka J. Math. **46** (2009), no. 3, 685–693. MR MR2583324

- [51] Carlos Rito, *Involutions on surfaces with  $p_g = q = 1$* , *Collectanea Mathematica* **61** (2010), no. 1, 81–106.
- [52] ———, *On equations of double planes with  $p_g = q = 1$* , *Math. Comp* **79** (2010), 1091–1108.
- [53] Maria Marti Sanchez, *Even sets of  $(-4)$ -curves on rational surface*, 2010.
- [54] Stefan Schröer, *Kummer surfaces for the self-product of the cuspidal rational curve*, *J. Algebraic Geom.* **16** (2007), no. 2, 305–346. MR MR2274516 (2007i:14038)
- [55] Matthias Schütt, Tetsuji Shioda, and Ronald van Luijk, *Lines on Fermat surfaces*, *J. Number Theory* **130** (2010), no. 9, 1939–1963.
- [56] James P Smith, *Picard-Fuchs differential equations for families of K3 surfaces*, Ph D thesis, University of Warwick, 2007.
- [57] Kaori Suzuki, *On Fano indices of  $Q$ -Fano 3-folds*, *Manuscripta Math.* **114** (2004), no. 2, 229–246. MR MR2067795 (2005c:14046)
- [58] Damiano Testa, Anthony Vårilly-Alvarado, and Mauricio Velasco, *Cox rings of degree one del Pezzo surfaces*, *Algebra and Number Theory* **3** (2009), 729–761.
- [59] Ronald van Luijk, *Quartic K3 surfaces without nontrivial automorphisms*, *Math. Res. Lett.* **13** (2006), no. 2-3, 423–439. MR MR2231128 (2007b:14084)
- [60] ———, *An elliptic K3 surface associated to Heron triangles*, *J. Number Theory* **123** (2007), no. 1, 92–119. MR MR2295433 (2007k:14077)
- [61] ———, *K3 surfaces with Picard number one and infinitely many rational points*, *Algebra and Number Theory* **1** (2007), no. 1, 1–15.
- [62] Anthony Vårilly-Alvarado, *Weak approximation on del Pezzo surfaces of degree 1*, *Adv. Math.* **219** (2008), no. 6, 2123–2145. MR MR2456278
- [63] Anthony Vårilly-Alvarado and Bianca Viray, *Failure of the Hasse principle for Enriques surfaces*, *Advances in Mathematics* **226** (2011), 4884–4901.
- [64] Anthony Vårilly-Alvarado and David Zywina, *Arithmetic  $E_8$  lattices with maximal Galois action*, *LMS J. Comput. Math.* **12** (2009), 144–165. MR MR2559115



- [65] Bogdan G. Vioreanu, *Mordell-Weil problem for cubic surfaces, numerical evidence*, 2008.
- [66] Bianca Viray, *A family of varieties with exactly one pointless rational fiber*, 2009.

# Abelian Varieties and Schemes

14Kxx

- [1] Nils Bruin, E. Victor Flynn, Josep González, and Victor Rotger, *On finiteness conjectures for endomorphism algebras of abelian surfaces*, Math. Proc. Cambridge Philos. Soc. **141** (2006), no. 3, 383–408. MR MR2281405
- [2] Robert Carls, David Kohel, and David Lubicz, *Higher-dimensional 3-adic CM construction*, J. Algebra **319** (2008), no. 3, 971–1006. MR MR2379090
- [3] John Cullinan, *Local-global properties of torsion points on three-dimensional abelian varieties*, J. Algebra **311** (2007), no. 2, 736–774. MR MR2314732 (2008b:14077)
- [4] Arsen Elkin and Yuri G. Zarhin, *Endomorphism algebras of hyperelliptic Jacobians and finite projective lines*, J. Ramanujan Math. Soc. **21** (2006), 169–187. MR MR2244543
- [5] Eyal Z. Goren and Kristin E. Lauter, *The distance between superspecial abelian varieties with real multiplication*, J. Number Theory **129** (2009), no. 6, 1562–1578. MR MR2521493
- [6] Hans-Christian Graf v. Bothmer, *Finite field experiments*, Higher-dimensional Geometry over Finite Fields, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., vol. 16, IOS, Amsterdam, 2008, pp. 1–62. MR MR2484075 (2009m:14032)
- [7] Everett W. Howe and Hui June Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory **92** (2002), no. 1, 139–163. MR MR1880590 (2003g:11063)
- [8] Rafe Jones and Jeremy Rouse, *Iterated endomorphisms of abelian algebraic groups*, Proc. London Math. Soc. **100** (2010), 763–794.
- [9] Gilles Lachaud and Christophe Ritzenthaler, *On a conjecture of Serre on abelian threefolds*, Algebraic Geometry and its applications, Proceedings of the First SAGA conference, Papeete, France 2007, 2008, pp. 1–28.
- [10] N. I. Shepherd-Barron, *Perfect forms and the moduli space of abelian varieties*, Invent. Math. **163** (2006), no. 1, 25–45. MR MR2208417

# Algebraic Groups

14Lxx

- [1] Thomas Bayer, *An algorithm for computing invariants of linear actions of algebraic groups up to a given degree*, J. Symbolic Comput. **35** (2003), no. 4, 441–449. MR MR1976577 (2004c:13045)
- [2] David J. Benson, Philip Bergonio, Brian D. Boe, Leonard Chastkofsky, Bobbe Cooper, Jeremiah Hower, Jo Jang Hyun, Jonathan Kujawa, Nadia Mazza, Daniel K. Nakano, Kenyon J. Platt, and Caroline Wright, *Support varieties for Weyl modules over bad primes*, J. Algebra **312** (2007), no. 2, 602–633.
- [3] Arjeh M. Cohen, Sergei Haller, and Scott H. Murray, *Computing in unipotent and reductive algebraic groups*, LMS J. Comput. Math. **11** (2008), 343–366. MR MR2452553
- [4] ———, *Computing with root subgroups of twisted reductive groups*, 2009.
- [5] Willem A. de Graaf, *Constructing algebraic groups from their Lie algebras*, J. Symbolic Comput. **44** (2009), no. 9, 1223–1233.
- [6] Michael Dettweiler and Stefan Reiter, *On exceptional rigid local systems*, 2006.
- [7] Ben Howard, John Millson, Andrew Snowden, and Ravi Vakil, *The ring of projective invariants of eight points on the line via representation theory*, 2008.
- [8] Benjamin Howard, John Millson, Andrew Snowden, and Ravi Vakil, *The equations for the moduli space of  $n$  points on the line*, Duke Math. J. **146** (2009), no. 2, 175–226. MR MR2477759 (2009m:14070)
- [9] Rafe Jones and Jeremy Rouse, *Galois theory of iterated endomorphisms*, Proc. London Math. Soc. (3) **100** (2010), 763–794.
- [10] P. I. Katsylo and V. L. Popov, *On fixed points of algebraic actions on  $\mathbf{C}^n$* , Funktsional. Anal. i Prilozhen. **34** (2000), no. 1, 41–50, 96. MR MR1756733 (2001c:14072)
- [11] Masanari Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447. MR MR2172348 (2007h:14061)
- [12] Stefan Maubach and Roel Willems, *Polynomial automorphisms over finite fields: Mimicking non-tame and tame maps by the Derksen group*, 2009.

- [13] Ian Morrison and David Swinarski, *Groebner techniques for low degree Hilbert stability*, 2009.
- [14] University of Georgia VIGRE Algebra Group, *Varieties of nilpotent elements for simple Lie algebras. II. Bad primes*, J. Algebra **292** (2005), no. 1, 65–99, The University of Georgia VIGRE Algebra Group: David J. Benson, Philip Bergonio, Brian D. Boe, Leonard Chastkofsky, Bobbe Cooper, G. Michael Guy, Jeremiah Hower, Markus Hunziker, Jo Jang Hyun, Jonathan Kujawa, Graham Matthews, Nadia Mazza, Daniel K. Nakano, Kenyon J. Platt and Caroline Wright. MR MR2166796
- [15] ———, *Support varieties for Weyl modules over bad primes*, J. Algebra **312** (2007), no. 2, 602–633, University of Georgia VIGRE Algebra Group: David J. Benson, Philip Bergonio, Brian D. Boe, Leonard Chastkofsky, Bobbe Cooper, Jeremiah Hower, Jo Jang Hyun, Jonathan Kujawa, Nadia Mazza, Daniel K. Nakano, Kenyon J. Platt and Caroline Wright. MR MR2333175
- [16] Stefan Schröer, *Kummer surfaces for the self-product of the cuspidal rational curve*, J. Algebraic Geom. **16** (2007), no. 2, 305–346. MR MR2274516 (2007i:14038)
- [17] Magda Sebestean, *Correspondance de McKay et Equivalences Derivees*, Ph.D. thesis, Paris VII, 2005, p. 169.
- [18] R. James Shank and David L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002), no. 4, 438–450. MR MR1897423 (2003a:13005)

# Special Varieties

14Mxx

- [1] Tatiana Bandman, Fritz Grunewald, Boris Kunyavskii, and Nathan Jones, *Geometry and arithmetic of verbal dynamical systems on simple groups*, Groups, Geometry, and Dynamics **4** (2010), no. 4, 607–655.
- [2] Christian Böhning, *The rationality of the moduli space of curves of genus 3 after P. Katsylo*, 2008.
- [3] Weronika Buczyńska, *Phylogenetic varieties on graphs*, 2010.
- [4] Jarosław Buczyński, *Legendrian subvarieties of projective space*, Geom. Dedicata **118** (2006), 87–103. MR MR2239450
- [5] Wouter Castryck and John Voight, *Nondegenerate curves of low genus over small finite fields*, Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 521, AMS, Providence, R.I., 2009, pp. 21–28.
- [6] Alessio Corti and Miles Reid, *Weighted Grassmannians*, Algebraic Geometry, de Gruyter, Berlin, 2002, pp. 141–163. MR MR1954062 (2003m:14076)
- [7] Ulrich Derenthal, *Universal torsors of del Pezzo surfaces and homogeneous spaces*, Adv. Math. **213** (2007), no. 2, 849–864. MR MR2332612
- [8] Johan P. Hansen, *Toric varieties, Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 4, 289–300. MR MR1953195 (2003j:14029)
- [9] Stephen P. Humphries, *Action of braid groups on determinantal ideals, compact spaces and a stratification of Teichmüller space*, Invent. Math. **144** (2001), no. 3, 451–505. MR MR1833891 (2002c:20056)
- [10] Michael Joswig and Nikolaus Witte, *Products of foldable triangulations*, Adv. Math. **210** (2007), no. 2, 769–796. MR MR2303239 (2008c:52017)
- [11] Stavros Argyrios Papadakis, *Type II unprojection*, J. Algebraic Geom. **15** (2006), no. 3, 399–414. MR MR2219843

- [12] Vladimir L. Popov, *Irregular and singular loci of commuting varieties*, Transform. Groups **13** (2008), no. 3-4, 819–837.
- [13] Miles Reid, *Examples of type IV unprojection*, 2001.
- [14] Diego Ruano, *On the parameters of  $r$ -dimensional toric codes*, Finite Fields Appl. **13** (2007), no. 4, 962–976. MR MR2360532
- [15] Helena Verrill and David Joyner, *Computing with toric varieties*, J. Symbolic Comput. **42** (2007), no. 5, 511–532. MR MR2322471 (2008e:68162)

# Real Algebraic Geometry

14Pxx

- [1] Bernd Bank, Marc Giusti, Joos Heintz, Mohab Safey El Din, and Eric Schost, *On the geometry of polar varieties*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 1, 33–83. MR 2585564
- [2] Saugata Basu and Michael Kettner, *Computing the Betti numbers of arrangements in practice*, Computer Algebra in Scientific Computing, Lecture Notes in Computer Science, vol. 3718, Springer Berlin/Heidelberg, 2005, pp. 13–31.
- [3] Mbakop Guy Merlin, *Eziente losung reeller polynomialer gleichungssysteme*, PhD Thesis, Humboldt-Universität, Berlin, 1999.
- [4] S. Petitjean, *Algebraic geometry and computer vision: Polynomial systems, real and complex roots*, J. Math. Imaging Vision **10** (1999), no. 3, 191–220. MR MR1695944 (2001e:68197)
- [5] Mohab Safey El Din, *Testing sign conditions on a multivariate polynomial and applications*, Math. Comput. Sci. **1** (2007), no. 1, 177–207. MR MR2384818
- [6] Mohab Safey El Din and Éric Schost, *Properness defects of projections and computation of at least one point in each connected component of a real algebraic set*, Discrete Comput. Geom. **32** (2004), no. 3, 417–430. MR MR2081634 (2005h:14136)

# Computational Methods

14-04, 14Qxx

- [1] Fatima K. Abu Salem and Kamal Khuri-Makdisi, *Fast Jacobian group operations for  $C_{3,4}$  curves over a large finite field*, LMS J. Comput. Math. **10** (2007), 307–328 (electronic). MR MR2335723
- [2] S. Arita, S. Miura, and T. Sekiguchi, *An addition algorithm on the Jacobian varieties of curves*, J. Ramanujan Math. Soc. **19** (2004), no. 4, 235–251. MR MR2125500 (2005m:14114)
- [3] Tobias Beck and Josef Schicho, *Adjoint computation for hypersurfaces using formal desingularizations*, J. Algebra **320** (2008), no. 11, 3984–3996. MR MR2464803 (2009k:14029)
- [4] ———, *Curve parametrization over optimal field extensions exploiting the Newton polygon*, Geometric Modeling and Algebraic Geometry, Springer, Berlin, 2008, pp. 119–140. MR MR2381607 (2009b:65032)
- [5] Gavin Brown, *A database of polarized K3 surfaces*, Experiment. Math. **16** (2007), no. 1, 7–20. MR MR2312974
- [6] Gavin Brown and Daniel Ryder, *Elliptic fibrations on cubic surfaces*, J. Pure Appl. Algebra **214** (2010), no. 4, 410–421. MR MR2558749
- [7] Gavin Brown and Kaori Suzuki, *Computing certain Fano 3-folds*, Japan J. Indust. Appl. Math. **24** (2007), no. 3, 241–250. MR MR2374989 (2008j:14076)
- [8] Laurent Busé and Marc Chardin, *Implicitizing rational hypersurfaces using approximation complexes*, J. Symbolic Comput. **40** (2005), no. 4-5, 1150–1168. MR MR2172855 (2006g:14097)
- [9] Gweltaz Chatel and David Lubicz, *A point counting algorithm using cohomology with compact support*, 2008.
- [10] David A. Cox, John Little, and Donal O’Shea, *Using Algebraic Geometry*, second ed., Graduate Texts in Mathematics, vol. 185, Springer, New York, 2005. MR MR2122859 (2005i:13037)



- [11] Willem A. de Graaf, *Constructing algebraic groups from their Lie algebras*, J. Symbolic Comput. **44** (2009), no. 9, 1223–1233.
- [12] Willem A. de Graaf, Michael Harrison, Jana Pílníková, and Josef Schicho, *A Lie algebra method for rational parametrization of Severi-Brauer surfaces*, J. Algebra **303** (2006), no. 2, 514–529. MR MR2255120 (2007e:14058)
- [13] Wolfram Decker and Christoph Lossen, *Computing in algebraic geometry*, Algorithms and Computation in Mathematics, vol. 16, Springer-Verlag, Berlin, 2006, A quick start using SINGULAR. MR MR2220403 (2007b:14129)
- [14] André Galligo and David Rupprecht, *Irreducible decomposition of curves*, J. Symbolic Comput. **33** (2002), no. 5, 661–677, Computer algebra (London, ON, 2001). MR MR1919909 (2003h:14091)
- [15] Ralf Gerkmann, Mao Sheng, and Kang Zuo, *Computational details on the disproof of modularity*, 2007.
- [16] Martine Girard and Leopoldo Kulesz, *Computation of sets of rational points of genus-3 curves via the Demjanenko-Manin method*, LMS J. Comput. Math. **8** (2005), 267–300 (electronic). MR MR2193214
- [17] Massimo Giulietti, *Algebraic curves over finite fields and MAGMA*, Ital. J. Pure Appl. Math. (2000), no. 8, 19–32. MR MR1793739 (2001i:14082)
- [18] Michael Harrison and Josef Schicho, *Rational parametrisation for degree 6 Del Pezzo surfaces using Lie algebras*, ISSAC 2006, ACM, New York, 2006, pp. 132–137. MR MR2289111
- [19] Hendrik Hubrechts, *Memory efficient hyperelliptic curve point counting*, 2006.
- [20] Gabriela Jeronimo, Teresa Krick, Juan Sabia, and Martín Sombra, *The computational complexity of the Chow form*, Found. Comput. Math. **4** (2004), no. 1, 41–117. MR MR2035410 (2005c:14083)
- [21] Tanja Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), no. 5, 295–328. MR MR2122308 (2005j:14082)
- [22] Alan G. B. Lauder, *A recursive method for computing zeta functions of varieties*, LMS J. Comput. Math. **9** (2006), 222–269 (electronic). MR MR2261044 (2007g:14022)

- [23] Walter D. Neumann and Penelope G. Wightwick, *Algorithms for polynomials in two variables*, Combinatorial and Computational Algebra (Hong Kong, 1999), Contemp. Math., vol. 264, Amer. Math. Soc., Providence, RI, 2000, pp. 219–235. MR MR1800698 (2002g:14091)
- [24] Jana Pílníková, *Parametrizing algebraic varieties using Lie algebras*, 2006.
- [25] Carlos Rito, *On equations of double planes with  $p_g = q = 1$* , Math. Comp **79** (2010), 1091–1108.
- [26] ———, *On the computation of singular plane curves and quartic surfaces*, 2010.
- [27] Mohab Safey El Din, *Testing sign conditions on a multivariate polynomial and applications*, Math. Comput. Sci. **1** (2007), no. 1, 177–207. MR MR2384818
- [28] Mohab Safey El Din and Éric Schost, *Properness defects of projections and computation of at least one point in each connected component of a real algebraic set*, Discrete Comput. Geom. **32** (2004), no. 3, 417–430. MR MR2081634 (2005h:14136)
- [29] Tanush Shaska, *Computational algebra and algebraic curves*, Comm. Comp. Alg. **37** (2003), no. 4, 117–124.
- [30] Dongming Wang, *Decomposing algebraic varieties*, Automated Deduction in Geometry (Beijing, 1998), Lecture Notes in Comput. Sci., vol. 1669, Springer, Berlin, 1999, pp. 180–206. MR MR1775951 (2001f:68144)

# Algebraic Structures

## Ordered Structures

06Xxx

- [1] Robin Christian, Marston Conder, and Arkadii Slinko, *Flippable pairs and subset comparisons in comparative probability orderings*, *Order* **24** (2007), no. 3, 193–213. MR MR2358081 (2008j:60048)
- [2] Marston Conder, Simon Marshall, and Arkadii Slinko, *Orders on multisets and discrete cones*, *Order* **24** (2007), no. 4, 277–296. MR MR2377917 (2008m:06045)

# Algebras – Associative

## Associative Algebras: General

16Bxx, 16Lxx, 16Nxx, 16Pxx

- [1] Noah Arbesfeld and David Jordan, *New results on the lower central series quotients of a free associative algebra*, J. Algebra **323** (2010), no. 6, 1813–1825. MR 2588142 (2011b:16085)
- [2] N. Bourbaki, *Algèbres tensorielles, algèbres extérieures, algèbres symétriques*, Algèbre, Bourbaki, Springer, 2007, pp. 379–596.
- [3] Galyna Dobrovolska, John Kim, and Xiaoguang Ma, *On the lower central series of an associative algebra (with an appendix by Pavel Etingof)*, J. Algebra **320** (2008), no. 1, 213–237. MR MR2417985
- [4] Ching-Hwa Eu and Travis Schedler, *Calabi-Yau Frobenius algebras*, J. Alg. **321** (2009), no. 3, 774–815.
- [5] Victor Ginzburg, *Calabi-Yau algebras*, 2007.
- [6] Robert Guralnick and Susan Montgomery, *Frobenius-Schur indicators for subgroups and the Drinfeld double of Weyl groups*, Trans. Amer. Math. Soc. **361** (2009), no. 7, 3611–3632. MR MR2491893
- [7] Max-Albert Knus and Jean-Pierre Tignol, *Triality and étale algebras*, Quadratic Forms, Linear Algebraic Groups, and Cohomology (Jean-Louis Colliot-Thélène, Skip Garibaldi, R. Sujatha, and Venapally Suresh, eds.), Developments in Mathematics, vol. 18, Springer New York, 2010, pp. 259–286.
- [8] Yi Sun, *Finite dimensional representations of the rational Cherednik algebra for  $G_4$* , J. Algebra **323** (2010), no. 10, 2864–2887. MR 2609179
- [9] John Voight, *Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms*, 2010.
- [10] Eliana Zoque, *A counterexample to the existence of a Poisson structure on a twisted group algebra*, 2006.

# Modules and Ideals

16Dxx, 16Exx

- [1] Martina Balagovic and Anirudha Balasubramanian, *On the lower central series quotients of a graded associative algebra*, J. Algebra **To appear** (2010).
- [2] Werner Bley and Stephen M. J. Wilson, *Computations in relative algebraic  $K$ -groups*, LMS J. Comput. Math. **12** (2009), 166–194. MR 2564571 (2010k:16013)
- [3] Edward L. Green and Øyvind Solberg, *An algorithmic approach to resolutions*, J. Symbolic Comput. **42** (2007), no. 11-12, 1012–1033. MR MR2368070 (2008i:16007)
- [4] Katsushi Waki, *Calculation of direct summands of  $FG$ -modules*, Sci. Rep. Hirosaki Univ. **44** (1997), no. 2, 193–200. MR MR1619001 (99c:16006)

# Representation Theory

16Gxx

- [1] Alexander Chistov, Gábor Ivanyos, and Marek Karpinski, *Polynomial time algorithms for modules over finite dimensional algebras*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI) (New York), ACM, 1997, pp. 68–74 (electronic). MR MR1809971
- [2] Galyna Dobrovolska and Pavel Etingof, *An upper bound for the lower central series quotients of a free associative algebra*, Int. Math. Res. Not. IMRN (2008), no. 12, Art. ID rnn039, 10. MR MR2426755
- [3] Pavel Etingof and Victor Ginzburg, *Noncommutative complete intersections and matrix integrals*, Pure Appl. Math. Q. **3** (2007), no. 1, part 3, 107–151. MR MR2330156 (2008b:16044)
- [4] Pavel Etingof, Alexei Oblomkov, and Eric Rains, *Generalized double affine Hecke algebras of rank 1 and quantized del Pezzo surfaces*, Adv. Math. **212** (2007), no. 2, 749–796. MR MR2329319
- [5] Edward L. Green, Lenwood S. Heath, and Craig A. Struble, *Constructing homomorphism spaces and endomorphism rings*, J. Symbolic Comput. **32** (2001), no. 1-2, 101–117, Computer algebra and mechanized reasoning (St. Andrews, 2000). MR MR1840387 (2002g:16019)
- [6] Sefi Ladkani, *On the periodicity of Coxeter transformations and the non-negativity of their Euler forms*, Linear Algebra Appl. **428** (2008), no. 4, 742–753. MR MR2382086 (2009b:16037)
- [7] Klaus M. Lux and Magdolna Szőke, *Computing homomorphism spaces between modules over finite dimensional algebras*, Experiment. Math. **12** (2003), no. 1, 91–98. MR MR2002676
- [8] ———, *Computing decompositions of modules over finite-dimensional algebras*, Experiment. Math. **16** (2007), no. 1, 1–6. MR MR2312973 (2008c:16020)
- [9] Craig A. Struble, *Analysis and implementation of algorithms for noncommutative algebra*, Ph.D. thesis, Virginia Polytechnic Institute and State University, 2000, p. 298.

# Orders and Arithmetic

16Hxx

- [1] Werner Bley and Henri Johnston, *Computing generators of free modules over orders in group algebras*, J. Algebra **320** (2008), no. 2, 836–852. MR MR2422318
- [2] Emmanuel Hallouin and Christian Maire, *Cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **595** (2006), 189–213. MR MR2244802 (2007g:11146)
- [3] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput **39** (2010), no. 5, 1714–1747.
- [4] John Voight, *Quadratic Forms and Quaternion Algebras: Algorithms and Arithmetic*, Ph.D. thesis, Berkeley, 2005, p. 98.

# Division Rings and Semisimple Artin Rings

16Kxx

- [1] Jana Pílníková, *Trivializing a central simple algebra of degree 4 over the rational numbers*, J. Symbolic Comput. **42** (2007), no. 6, 579–586. MR MR2325916 (2008c:16030)



# Algebras from Standard Constructions

16Sxx

- [1] Jon F. Carlson and Graham Matthews, *Generators and relations for matrix algebras*, J. Algebra **300** (2006), no. 1, 134–159. MR MR2228640
- [2] Robert S. Coulter, George Havas, and Marie Henderson, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's  $p^s$ -polynomials*, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput, vol. 9, World Sci. Publ., River Edge, NJ, 2001, pp. 36–45. MR MR1877440 (2002m:11103)
- [3] Galyna Dobrovolska and Pavel Etingof, *An upper bound for the lower central series quotients of a free associative algebra*, Int. Math. Res. Not. IMRN (2008), no. 12, Art. ID rnn039, 10. MR MR2426755
- [4] Pavel Etingof and Victor Ginzburg, *Noncommutative complete intersections and matrix integrals*, Pure Appl. Math. Q. **3** (2007), no. 1, part 3, 107–151. MR MR2330156 (2008b:16044)
- [5] Pavel Etingof, John Kim, and Xiaoguang Ma, *On universal Lie nilpotent associative algebras*, J. Algebra **321** (2009), no. 2, 697–703. MR MR2483288 (2010d:16029)
- [6] Boris Feigin and Boris Shoikhet, *On  $[A, A]/[A, [A, A]]$  and on a  $W_n$ -action on the consecutive commutators of free associative algebra*, Math. Res. Lett. **14** (2007), no. 5, 781–795. MR MR2350124 (2009b:16055)
- [7] Edward L. Green, Lenwood S. Heath, and Craig A. Struble, *Constructing endomorphism rings via duals*, ISSAC '00: Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews) (New York), ACM, 2000, pp. 129–136 (electronic). MR MR1805116 (2003b:16031)
- [8] ———, *Constructing homomorphism spaces and endomorphism rings*, J. Symbolic Comput. **32** (2001), no. 1-2, 101–117, Computer algebra and mechanized reasoning (St. Andrews, 2000). MR MR1840387 (2002g:16019)
- [9] Timo Hanke, *A twisted Laurent series ring that is a noncrossed product*, Israel J. Math. **150** (2005), 199–203. MR MR2255807

- [10] Miles Lee Holloway, *Derived equivalences for group algebras*, Dissertation, University of Bristol, 2001.
- [11] Brent Kerby, *Automorphism groups of Schur rings*, 2009.
- [12] R. V. Kravchenko and B. V. Petrenko, *Some formulas for the minimal number of generators of the direct sum of matrix rings*, 2007.
- [13] Matthias Külzner, *On representations of twisted group rings*, J. Group Theory **7** (2004), no. 2, 197–229. MR MR2049017 (2005h:20004)
- [14] M. Anwar Rao and Robert Sandling, *The characterisation of modular group algebras having unit groups of nilpotency class 3*, Canad. Math. Bull. **38** (1995), no. 1, 112–116. MR MR1319908 (96c:16044)
- [15] I. K. Redchuk, *Finite-dimensionality and growth of algebras defined by polylinearly connected generators*, Ukrain. Mat. Zh. **57** (2005), no. 10, 1435–1440. MR MR2220096 (2007b:16046)
- [16] Robert Sandling, *Presentations for unit groups of modular group algebras of groups of order 16*, Math. Comp. **59** (1992), no. 200, 689–701. MR MR1136226 (93a:16025)
- [17] Stewart Wilcox, *Complementation in the group of units of matrix rings*, Bull. Austral. Math. Soc. **70** (2004), no. 2, 223–227. MR MR2094290 (2005f:16055)

# Computational Methods

16-04

- [1] Werner Bley and Henri Johnston, *Computing generators of free modules over orders in group algebras*, J. Algebra **320** (2008), no. 2, 836–852. MR MR2422318
- [2] Jon F. Carlson and Graham Matthews, *Generators and relations for matrix algebras*, J. Algebra **300** (2006), no. 1, 134–159. MR MR2228640
- [3] Alexander Chistov, Gábor Ivanyos, and Marek Karpinski, *Polynomial time algorithms for modules over finite dimensional algebras*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI) (New York), ACM, 1997, pp. 68–74 (electronic). MR MR1809971
- [4] David J. Green, *Gröbner bases for  $p$ -group algebras*, 2009.
- [5] Edward L. Green, Lenwood S. Heath, and Craig A. Struble, *Constructing homomorphism spaces and endomorphism rings*, J. Symbolic Comput. **32** (2001), no. 1-2, 101–117, Computer algebra and mechanized reasoning (St. Andrews, 2000). MR MR1840387 (2002g:16019)
- [6] Timo Hanke, *The isomorphism problem for cyclic algebras and an application*, ISSAC 2007, ACM, New York, 2007, pp. 181–186. MR MR2396201 (2009d:16026)
- [7] Gábor Ivanyos and Klaus Lux, *Treating the exceptional cases of the MeatAxe*, Experiment. Math. **9** (2000), no. 3, 373–381. MR MR1795309 (2001j:16067)
- [8] Graham Matthews, *Computing Generators and Relations for Matrix Algebras*, PhD Thesis, University of Georgia, 2004.
- [9] Gabriele Nebe and Allan Steel, *Recognition of division algebras*, J. Algebra **322** (2009), no. 3, 903–909.
- [10] Bernd Souvignier, *Decomposing homogeneous modules of finite groups in characteristic zero*, J. Algebra **322** (2009), no. 3, 948–956.
- [11] John Voight, *Identifying the matrix ring: Algorithms for quaternion algebras and quadratic forms*, 2010.

- [12] Katsushi Waki, *Calculation of direct summands of FG-modules*, Sci. Rep. Hirosaki Univ. **44** (1997), no. 2, 193–200. MR MR1619001 (99c:16006)

# Algebras – Non-Associative

## Nonassociative Algebras: General

17Axx

- [1] Vyacheslav A. Artamonov, Alexander A. Mikhalev, and Alexander V. Mikhalev, *Combinatorial properties of free algebras of Schreier varieties*, Polynomial identities and combinatorial methods (Pantelleria, 2001), Lecture Notes in Pure and Appl. Math., vol. 235, Dekker, New York, 2003, pp. 47–99. MR MR2021795 (2004j:17001)
- [2] Antonio Behn, Alberto Elduque, and Alicia Labra, *A class of locally nilpotent commutative algebras*, 2009.
- [3] Christopher P. Bendel, Daniel K. Nakano, and Cornelius Pillen, *Second cohomology groups for Frobenius kernels and related structures*, Adv. Math. **209** (2007), no. 1, 162–197. MR MR2294220 (2008c:20085)
- [4] Kelly McKinnie, *Indecomposable  $p$ -algebras and Galois subfields in generic abelian crossed products*, J. Algebra **320** (2008), no. 5, 1887–1907. MR MR2437635
- [5] L. J. Rylands and D. E. Taylor, *Constructions for octonion and exceptional Jordan algebras*, Des. Codes Cryptogr. **21** (2000), no. 1-3, 191–203. MR MR1801200 (2001m:17022)
- [6] Donald E. Taylor, *Constructing the split octonions*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 161–185. MR MR2278927
- [7] Mikael Vejdemo-Johansson, *Blackbox computation of  $A_\infty$ -algebras*, Georgian Journal of Mathematics **To appear** (2010).

# Lie Algebras

17Bxx except 17B37

- [1] Y. Barnea and D. S. Passman, *Filtrations in semisimple Lie algebras. II*, Trans. Amer. Math. Soc. **360** (2008), no. 2, 801–817 (electronic). MR MR2346472 (2008m:17016)
- [2] Laurent Bartholdi, Benjamin Enriquez, Pavel Etingof, and Eric Rains, *Groups and Lie algebras corresponding to the Yang-Baxter equations*, J. Algebra **305** (2006), no. 2, 742–764. MR MR2266850
- [3] Dietrich Burde, Bettina Eick, and Willem de Graaf, *Computing faithful representations for nilpotent Lie algebras*, J. Algebra **322** (2009), no. 3, 602–612. MR MR2531213
- [4] A. Caranti, S. Mattarei, and M. F. Newman, *Graded Lie algebras of maximal class*, Trans. Amer. Math. Soc. **349** (1997), no. 10, 4021–4051. MR MR1443190 (98a:17027)
- [5] A. Caranti and M. F. Newman, *Graded Lie algebras of maximal class. II*, J. Algebra **229** (2000), no. 2, 750–784. MR MR1769297 (2001g:17041)
- [6] Serena Cicalò and Willem A. de Graaf, *Non-associative Gröbner bases, finitely-presented Lie rings and the Engel condition: II*, J. Symbolic Comput. **44** (2009), no. 7, 786–800.
- [7] Arjeh M. Cohen and Dan Roozemon, *Computing Chevalley bases in small characteristics*, J. Algebra **322** (2009), no. 3, 703–721. MR MR2531218 (2010d:17025)
- [8] Jennifer R. Daniel and Aloysius G. Helminck, *Algorithms for computations in local symmetric spaces*, Comm. Algebra **36** (2008), no. 5, 1758–1788. MR MR2424265
- [9] W. A. de Graaf, *Using Cartan subalgebras to calculate nilradicals and Levi subalgebras of Lie algebras*, J. Pure Appl. Algebra **139** (1999), no. 1–3, 25–39, Effective methods in algebraic geometry (Saint-Malo, 1998). MR MR1700536 (2000j:17001)
- [10] Willem A. de Graaf, *Classification of solvable Lie algebras*, Experiment. Math. **14** (2005), no. 1, 15–25. MR MR2146516 (2006b:17019)
- [11] ———, *Classification of 6-dimensional nilpotent Lie algebras over fields of characteristic not 2*, J. Algebra **309** (2007), no. 2, 640–653. MR MR2303198 (2007k:17012)

- [12] Claus Fieker and Willem A. de Graaf, *Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras*, LMS J. Comput. Math. **10** (2007), 271–287 (electronic). MR MR2320832 (2008f:11119)
- [13] Conrad Kobel, *On the classification of solvable Lie algebras of finite dimension containing an abelian ideal of codimension one*, Master’s thesis, Halmstad University, 2008, p. 48.
- [14] L. G. Kovács and Ralph Stöhr, *Lie powers of the natural module for  $GL(2)$* , J. Algebra **229** (2000), no. 2, 435–462. MR MR1769283 (2001h:20070)
- [15] G.I. Lehrer and R.B. Zhang, *A Temperley-Lieb analogue for the BMW algebra*, 2008.
- [16] Sandro Mattarei and Marina Avitabile, *Diamonds of finite type in thin Lie algebras*, J. Lie Theory **19** (2009), no. 1, 431–439.
- [17] M. F. Newman and Michael Vaughan-Lee, *Engel-4 groups of exponent 5. II. Orders*, Proc. London Math. Soc. (3) **79** (1999), no. 2, 283–317. MR MR1702244 (2000e:20065)
- [18] University of Georgia VIGRE Algebra Group, *On Kostant’s theorem for Lie algebra cohomology*, Lin, Zongzhu (ed.) et al., Representation Theory. Fourth International Conference on Representation Theory, Lhasa, China, July 16–20, 2007., Contemporary Mathematics, vol. 478, American Mathematical Society (AMS), Providence, RI, 2009, pp. 39–60. MR )
- [19] Roman O. Popovych, Vyacheslav M. Boyko, Maryna O. Nesterenko, and Maxim W. Lutfullin, *Realizations of real low-dimensional Lie algebras*, J. Phys. A **36** (2003), 7337–7360.
- [20] S. M. Salamon, *Complex structures on nilpotent Lie algebras*, J. Pure Appl. Algebra **157** (2001), no. 2-3, 311–333. MR MR1812058 (2002g:53089)
- [21] H. Strade, *Lie algebras of small dimension*, Lie algebras, vertex operator algebras and their applications, Contemp. Math., vol. 442, Amer. Math. Soc., Providence, RI, 2007, pp. 233–265. MR MR2372566 (2009a:17027)
- [22] Michael Vaughan-Lee, *Simple Lie algebras of low dimension over  $GF(2)$* , LMS J. Comput. Math. **9** (2006), 174–192 (electronic). MR MR2237261
- [23] Geordie Williamson, *Intersection cohomology complexes on low rank flag varieties*, 2007.

- [24] Eliana Zoque, *A counterexample to the existence of a Poisson structure on a twisted group algebra*, 2006.



# Quantum Groups

17B37

- [1] Laurent Bartholdi, Benjamin Enriquez, Pavel Etingof, and Eric Rains, *Groups and Lie algebras corresponding to the Yang-Baxter equations*, J. Algebra **305** (2006), no. 2, 742–764. MR MR2266850
- [2] C. P. Bendel, D. K. Nakano, B. J. Parshall, and C. Pillen, *Cohomology for quantum groups via the geometry of the Nullcone*, 2007, pp. 1–58.
- [3] Pavel Etingof and Victor Ginzburg, *Noncommutative complete intersections and matrix integrals*, Pure Appl. Math. Q. **3** (2007), no. 1, part 3, 107–151. MR MR2330156 (2008b:16044)
- [4] Julia Galstad and Gerald Hoehn, *A new class of codes over  $Z_2 \times Z_2$* , 2010.
- [5] Jan E. Grabowski, *Examples of quantum cluster algebras associated to partial flag varieties*, J. Pure Appl. Algebra **To appear** (2010).
- [6] Jan E. Grabowski and Stéphane Launois, *Quantum cluster algebra structures on quantum Grassmannians and their quantum Schubert cells: The finite-type cases*, Int.Math.Res. Not **To appear** (2010).

# Computational Methods

17-04

- [1] Serena Cicalò and Willem A. de Graaf, *Non-associative Gröbner bases, finitely-presented Lie rings and the Engel condition: II*, J. Symbolic Comput. **44** (2009), no. 7, 786–800.
- [2] W. A. de Graaf, *Using Cartan subalgebras to calculate nilradicals and Levi subalgebras of Lie algebras*, J. Pure Appl. Algebra **139** (1999), no. 1–3, 25–39, Effective methods in algebraic geometry (Saint-Malo, 1998). MR MR1700536 (2000j:17001)
- [3] Willem A. de Graaf, *Deciding isomorphism of Lie algebras*, Proceedings of the Sixth Rhine Workshop on Computer Algebra, Sankt Augustin, March 31 - April 3, 1998, 1998, p. 9.
- [4] ———, *Lie Algebras: Theory and Algorithms*, North-Holland Mathematical Library, vol. 56, North-Holland Publishing Co., Amsterdam, 2000. MR MR1743970 (2001j:17011)
- [5] Lothar Gerritzen, *Tree polynomials and non-associative Gröbner bases*, J. Symbolic Comput. **41** (2006), no. 3-4, 297–316. MR MR2202553 (2006k:17005)
- [6] Roberto La Scala and Viktor Levandovskyy, *Letterplace ideals and non-commutative Gröbner bases*, J. Symbolic Comp. **44** (2009), no. 10, 1374–1393.

# Analysis

## Analysis: General

26Xxx

- [1] Michael Clausen, *Fast Fourier transforms for metabelian groups*, SIAM J. Comput. **18** (1989), no. 3, 584–593. MR MR996838 (90e:94002)
- [2] Jeffrey B. Farr and Shuhong Gao, *Gröbner bases and generalized Padé approximation*, Math. Comp. **75** (2006), no. 253, 461–473 (electronic). MR MR2176409
- [3] Jean-Charles Faugère, François Moreau de Saint-Martin, and Fabrice Rouillier, *Design of regular nonseparable bidimensional wavelets using Gröbner basis techniques*, IEEE Trans. Signal Process. **46** (1998), no. 4, 845–856. MR MR1665643
- [4] M. Kasatani, T. Miwa, A. N. Sergeev, and A. P. Veselov, *Coincident root loci and Jack and Macdonald polynomials for special values of the parameters*, Jack, Hall-Littlewood and Macdonald Polynomials, Contemp. Math., vol. 417, Amer. Math. Soc., Providence, RI, 2006, pp. 207–225. MR MR2284129
- [5] Kiran S. Kedlaya, *Search techniques for root-unitary polynomials*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 71–81. MR MR2459990 (2009h:26022)
- [6] A. J. Scott and M. Grassl, *Symmetric informationally complete positive-operator-valued measures: A new computer study*, 2010, p. 042203.
- [7] J.C van der Meer, *Generic one-parameter versal unfoldings of symmetric hamiltonian systems in 1 : 1 resonance*, Int. J. Pure Appl. Math **53** (2009), no. 4, 547–561.
- [8] Shayne Waldron and Nick Hay, *On computing all harmonic frames of  $n$  vectors in  $C^d$* , Appl. Comput. Harmon. Anal. **21** (2006), no. 2, 168–181. MR MR2259777

# Riemann Surfaces

30Fxx

- [1] Alin Bostan, Manuel Kauers, and Mark van Hoeij, *The complete generating function for Gessel walks is algebraic*, Proc. Amer. Math. Soc. **138** (2010), no. 9, 3063–3078.
- [2] E. Bujalance, F. J. Cirre, M. D. E. Conder, and B. Szepietowski, *Finite group actions on bordered surfaces of small genus*, J. Pure Appl. Algebra **214** (2010), no. 12, 2165–2185. MR 2660907
- [3] E. Bujalance, Marston Conder, J. M. Gamboa, G. Gromadzki, and M. Izquierdo, *Double coverings of Klein surfaces by a given Riemann surface*, J. Pure Appl. Algebra **169** (2002), no. 2-3, 137–151. MR MR1897339 (2003e:14023)
- [4] Emilio Bujalance, F. J. Cirre, and Marston Conder, *On extendability of group actions on compact Riemann surfaces*, Trans. Amer. Math. Soc. **355** (2003), no. 4, 1537–1557 (electronic). MR MR1946404 (2003k:20079)
- [5] Emilio Bujalance and Marston Conder, *On cyclic groups of automorphisms of Riemann surfaces*, J. London Math. Soc. (2) **59** (1999), no. 2, 573–584. MR MR1709666 (2000g:20098)
- [6] Jason Callahan, *Jorgensen number and arithmeticity*, Conform. Geom. Dyn **13** (2009), 160–186.
- [7] Jason Todd Callahan, *The arithmetic and geometry of two-generator Kleinian groups*, Phd, University of Texas at Austin, 2009.
- [8] Marston Conder, *The genus of compact Riemann surfaces with maximal automorphism group*, J. Algebra **108** (1987), no. 1, 204–247. MR MR887205 (88f:20063)
- [9] ———, *Maximal automorphism groups of symmetric Riemann surfaces with small genus*, J. Algebra **114** (1988), no. 1, 16–28. MR MR931896 (89c:20049)
- [10] ———, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370. MR MR1041434 (91d:20032)
- [11] Marston Conder, C. Maclachlan, G. J. Martin, and E. A. O’Brien, *2-generator arithmetic Kleinian groups. III*, Math. Scand. **90** (2002), no. 2, 161–179. MR MR1895609 (2003b:20071)

- [12] Marston Conder and Gaven J. Martin, *Cusps, triangle groups and hyperbolic 3-folds*, J. Austral. Math. Soc. Ser. A **55** (1993), no. 2, 149–182. MR MR1232754 (94e:57018)
- [13] Robert Guralnick and John Shareshian, *Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points*, Mem. Amer. Math. Soc. **189** (2007), no. 886, vi+128, With an appendix by Guralnick and R. Stafford. MR MR2343794
- [14] Stephen P. Humphries, *Action of braid groups on determinantal ideals, compact spaces and a stratification of Teichmüller space*, Invent. Math. **144** (2001), no. 3, 451–505. MR MR1833891 (2002c:20056)
- [15] Sadok Kallel and Denis Sjerve, *On the group of automorphisms of cyclic covers of the Riemann sphere*, Math. Proc. Cambridge Philos. Soc. **138** (2005), no. 2, 267–287. MR MR2132169 (2006c:20106)
- [16] C. Maclachlan and G. J. Martin, *The non-compact arithmetic generalised triangle groups*, Topology **40** (2001), no. 5, 927–944. MR MR1860535 (2002i:30055)
- [17] Coy L. May, *The real genus of 2-groups*, J. Algebra Appl. **6** (2007), no. 1, 103–118. MR MR2302697 (2007m:30057)
- [18] Reza Zomorrodian, *On a theorem of supersoluble automorphism groups*, Proc. Amer. Math. Soc. **131** (2003), no. 9, 2711–2713 (electronic). MR MR1974326 (2004d:20060)

# Functions of Several Complex Variables

32Xxx

- [1] Pavel Etingof, André Henriques, Joel Kamnitzer, and Eric Rains, *The cohomology ring of the real locus of the moduli space of stable curves of genus 0 with marked points*, *Annals of Mathematics* **171** (2010), no. 2, 731–777.
- [2] Stephen P. Humphries, *Free products in mapping class groups generated by Dehn twists*, *Glasgow Math. J.* **31** (1989), no. 2, 213–218. MR MR997819 (90e:57024)
- [3] S. M. Salamon, *Complex structures on nilpotent Lie algebras*, *J. Pure Appl. Algebra* **157** (2001), no. 2-3, 311–333. MR MR1812058 (2002g:53089)

# Ordinary Differential Equations

34Xxx

- [1] Philip Boalch, *Some explicit solutions to the Riemann-Hilbert problem*, 2005.
- [2] Philip Boalch, *Higher genus icosahedral Painlevé curves*, Funk. Ekvac. (Kobe), **50** (2007), 19–32.
- [3] A. Bostan, F. Chyzak, F. Ollivier, B. Salvy, É. Schost, and A. Sedoglavic, *Fast computation of power series solutions of systems of differential equations*, SODA '07: Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms (Philadelphia, PA, USA), Society for Industrial and Applied Mathematics, 2007, pp. 1012–1021.
- [4] Alin Bostan, Thomas Cluzeau, and Bruno Salvy, *Fast algorithms for polynomial solutions of linear differential equations*, ISSAC'05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 45–52 (electronic). MR MR2280528
- [5] Delphine Boucher, Philippe Gaillard, and Felix Ulmer, *Fourth order linear differential equations with imprimitive group*, ISSAC '03: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2003, pp. 45–49 (electronic). MR MR2035193 (2004m:34201)
- [6] Olivier Cormier, *On Liouvillian solutions of linear differential equations of order 4 and 5*, ISSAC '01: Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2001, pp. 93–100 (electronic). MR MR2049736
- [7] Christopher M. Cosgrove, *Chazy classes IX–XI of third-order differential equations*, Stud. Appl. Math. **104** (2000), no. 3, 171–228. MR MR1752309 (2001d:34148)
- [8] Freddy Dumortier, Jaume Llibre, and Joan C. Artés, *Qualitative Theory of Planar Differential Systems*, Universitext, Springer-Verlag, Berlin, 2006. MR MR2256001
- [9] Winfried Fakler, *Algorithmen zur symbolischen lösung homogener linearer differentialgleichungen*, Diplomarbeit, Universität Karlsruhe, 1994.

- [10] Chris M. Field and Chris M. Ormerod, *An ultradiscrete matrix version of the fourth Painlevé equation*, Adv. Difference Equ. (2007), Art. ID 96752, 14. MR MR2322484 (2008d:39021)
- [11] Armengol Gasull and Joan Torregrosa, *A relation between small amplitude and big limit cycles*, Rocky Mountain J. Math. **31** (2001), no. 4, 1277–1303. MR MR1895296 (2002m:34037)
- [12] Jaume Giné and Xavier Santallusia, *Implementation of a new algorithm of computation of the Poincaré-Liapunov constants*, J. Comput. Appl. Math. **166** (2004), no. 2, 465–476. MR MR2041193 (2005d:34061)
- [13] Sabrina A. Hessinger, *Computing the Galois group of a linear differential equation of order four*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 489–536. MR MR1831942 (2002c:12009)
- [14] V.A. Krasikov and T.M. Sadykov, *Linear differential operators for generic algebraic curves*, 2010.
- [15] Sonja Lauer, *Entwurf von Algorithmen zur Konstruktion von Differentialgleichungen mit vorgegebener endlicher Galoisgruppe*, Diplomarbeit, Universität Karlsruhe, 2005.
- [16] Sonja Lauer, *Entwurf von Algorithmen zur Konstruktion von Differentialgleichungen mit vorgegebener endlicher Galoisgruppe*, Ph.D. thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 2006, p. 139.
- [17] Stefan Mărușter, Viorel Negru, Dana Petcu, and Călin Sandru, *Intelligent front-end for solving differential and non-linear equations systems*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **258** (1999), no. Teor. Predst. Din. Sist. Komb. i Algoritm. Metody. 4, 318–334, 361. MR MR1755844 (2001a:34001)
- [18] Michael F. Singer, *Testing reducibility of linear differential operators: A group-theoretic perspective*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 2, 77–104. MR MR1462491 (98e:12007)
- [19] Michael F. Singer and Felix Ulmer, *Galois groups of second and third order linear differential equations*, J. Symbolic Comput. **16** (1993), no. 1, 9–36. MR MR1237348 (94i:34015)
- [20] ———, *Liouvillian and algebraic solutions of second and third order linear differential equations*, J. Symbolic Comput. **16** (1993), no. 1, 37–73. MR MR1237349 (94i:34016)



- [21] ———, *On a third order differential equation whose differential Galois group is the simple group of 168 elements*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 316–324. MR MR1251988 (95e:34010)
- [22] ———, *Necessary conditions for Liouvillian solutions of (third order) linear differential equations*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), no. 1, 1–22. MR MR1341890 (96j:34005)
- [23] Felix Ulmer, *On algebraic solutions of linear differential equations with primitive unimodular Galois group*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (New Orleans, LA, 1991), Lecture Notes in Comput. Sci., vol. 539, Springer, Berlin, 1991, pp. 446–455. MR MR1229340 (94e:68094)
- [24] ———, *On Liouvillian solutions of linear differential equations*, Appl. Algebra Engrg. Comm. Comput. **2** (1992), no. 3, 171–193. MR MR1325527 (96e:12007)
- [25] ———, *Liouvillian solutions of third order differential equations*, J. Symbolic Comput. **36** (2003), no. 6, 855–889. MR MR2021282 (2004k:34007)

# Partial Differential Equations

35Xxx

- [1] Victor A. Galaktionov and Sergey R. Svirshchevskii, *Exact solutions and invariant subspaces of nonlinear partial differential equations in mechanics and physics*, Chapman & Hall/CRC Applied Mathematics and Nonlinear Science Series, Chapman & Hall/CRC, Boca Raton, FL, 2007. MR MR2272794 (2007j:35002)
- [2] Vladimir P. Gerdt, Yuri A. Blinkov, and Vladimir V. Mozzhilkin, *Gröbner bases and generation of difference schemes for partial differential equations*, SIGMA Symmetry Integrability Geom. Methods Appl. **2** (2006), Paper 051, 26 pp. (electronic). MR MR2240724
- [3] V.A. Krasikov and T.M. Sadykov, *Linear differential operators for generic algebraic curves*, 2010.
- [4] Ariane Péladan-Germa, *Testing equality in differential ring extensions defined by PDE's and limit conditions*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 4, 257–288. MR MR1953194 (2003k:12010)
- [5] Roman O. Popovych, Vyacheslav M. Boyko, Maryna O. Nesterenko, and Maxim W. Lutfullin, *Realizations of real low-dimensional Lie algebras*, J. Phys. A **36** (2003), 7337–7360.

# Dynamical Systems

37Xxx

- [1] David H. Bailey, Jonathan M. Borwein, Vishaal Kapoor, and Eric W. Weisstein, *Ten problems in experimental mathematics*, Amer. Math. Monthly **113** (2006), no. 6, 481–509. MR MR2231135 (2007b:65001)
- [2] Tatiana Bandman, Fritz Grunewald, Boris Kunyavskii, and Nathan Jones, *Geometry and arithmetic of verbal dynamical systems on simple groups*, Groups, Geometry, and Dynamics **4** (2010), no. 4, 607–655.
- [3] Wieb Bosma, Karma Dajani, and Cor Kraaikamp, *Entropy quotients and correct digits in number-theoretic expansions*, Dynamics and Stochastics, IMS Lecture Notes Monogr. Ser., vol. 48, Inst. Math. Statist., Beachwood, OH, 2006, pp. 176–188. MR MR2306199
- [4] Roberto Conti, Jason Kimberley, and Wojciech Szymanski, *More localized automorphisms of the Cuntz algebras*, 2008.
- [5] Ana Paula S. Dias, Benoit Dionne, and Ian Stewart, *Heteroclinic cycles and wreath product symmetries*, Dyn. Stab. Syst. **15** (2000), no. 4, 353–385. MR MR1809211 (2002b:37082)
- [6] ———, *Heteroclinic cycles and wreath product symmetries*, Symmetry and perturbation theory (Cala Gonone, 2001), World Sci. Publ., River Edge, NJ, 2001, pp. 53–57. MR MR1875466
- [7] Freddy Dumortier, Jaume Llibre, and Joan C. Artés, *Qualitative Theory of Planar Differential Systems*, Universitext, Springer-Verlag, Berlin, 2006. MR MR2256001
- [8] Soren Eilers and Ian Kiming, *On some new invariants for strong shift equivalence for shifts of finite type*, 2008.
- [9] Xander Faber, Benjamin Hutz, Patrick Ingram, Rafe Jones, Michelle Manes, Thomas J. Tucker, and Michael E. Zieve, *Uniform bounds on pre-images under quadratic dynamical systems*, Math. Res. Lett. **16** (2009), no. 1, 87–101. MR MR2480563

- [10] Karin Gatermann, *Computer algebra methods for equivariant dynamical systems*, Lecture Notes in Mathematics, vol. 1728, Springer-Verlag, Berlin, 2000. MR MR1755001 (2001k:37040)
- [11] Evelyn L. Hart and Edward C. Keppelmann, *Nielsen periodic point theory for periodic maps on orientable surfaces*, Topology Appl. **153** (2006), no. 9, 1399–1420. MR MR2211207 (2006m:55007)
- [12] Stephen Humphries and Anthony Manning, *Curves of fixed points of trace maps*, Ergodic Theory Dynam. Systems **27** (2007), no. 4, 1167–1198. MR MR2342971
- [13] Patrick Ingram, *Cubic polynomials with periodic cycles of a specified multiplier*, 2009.
- [14] Ole Lund Jensen, *Symbolic dynamic systems and their invariants*, Diplomarbeit, University of Copenhagen, 2002.
- [15] Jason S. Kimberley and Guyan Robertson, *Groups acting on products of trees, tiling systems and analytic  $K$ -theory*, New York J. Math. **8** (2002), 111–131 (electronic). MR MR1923572 (2003j:20042)
- [16] I. S. Kotsireas and K. Karamanos, *Exact computation of the bifurcation point  $B_4$  of the logistic map and the Bailey-Broadhurst conjectures*, Internat. J. Bifur. Chaos Appl. Sci. Engrg. **14** (2004), no. 7, 2417–2423. MR MR2087501 (2006c:37037)
- [17] Jeffrey C. Lagarias and Eric Rains, *Dynamics of a family of piecewise-linear area-preserving plane maps. II. Invariant circles*, J. Difference Equ. Appl. **11** (2005), no. 13, 1137–1163. MR MR2183011
- [18] Alina Ostafe and Igor E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, 2010.
- [19] David Pask, Iain Raeburn, and Natasha A. Weaver, *A family of 2-graphs arising from two-dimensional subshifts*, Ergodic Theory Dynam. Systems **29** (2009), no. 5, 1613–1639. MR MR2545020

# Operator Algebras

46Lxx

- [1] Roberto Conti, Jason Kimberley, and Wojciech Szymanski, *More localized automorphisms of the Cuntz algebras*, 2008.
- [2] Roberto Conti and Wojciech Szymanski, *Labeled trees and localized automorphisms of the Cuntz algebras*, 2008.
- [3] Jason S. Kimberley and Guyan Robertson, *Groups acting on products of trees, tiling systems and analytic K-theory*, New York J. Math. **8** (2002), 111–131 (electronic). MR MR1923572 (2003j:20042)
- [4] David Pask, Iain Raeburn, and Natasha A. Weaver, *A family of 2-graphs arising from two-dimensional subshifts*, Ergodic Theory Dynam. Systems **29** (2009), no. 5, 1613–1639. MR MR2545020
- [5] David Penneys, *A cyclic approach to the annular Temperley-Lieb category*, 2009.
- [6] Francesco Dalla Piazza, *More on superstring chiral measures*, Nuclear Physics B **844** (2011), no. 3, 471–499.
- [7] Guyan Robertson, *Torsion in boundary coinvariants and K-theory for affine buildings*, K-Theory **33** (2005), no. 4, 347–369. MR MR2220525
- [8] Guyan Robertson and Tim Steger, *Asymptotic K-theory for groups acting on  $A_2$  buildings*, Canad. J. Math. **53** (2001), no. 4, 809–833. MR MR1848508 (2002f:46141)

# Category Theory

## All Areas

18Xxx

- [1] Matthias Künzer, *Nonisomorphic Verdier octahedra on the same base*, J. Homotopy Relat. Struct. **4** (2009), no. 1, 7–38. MR MR2520985
- [2] David Penneys, *A cyclic approach to the annular Temperley-Lieb category*, 2009.

# Combinatorics

## Enumerative Combinatorics

05Axx

- [1] Alin Bostan, Manuel Kauers, and Mark van Hoeij, *The complete generating function for Gessel walks is algebraic*, Proc. Amer. Math. Soc. **138** (2010), no. 9, 3063–3078.
- [2] Peter J. Cameron, *Partitions and permutations*, Discrete Math. **291** (2005), no. 1-3, 45–54. MR MR2124054 (2005k:20003)
- [3] Philippe Cara, Serge Lehman, and Dmitrii V. Pasechnik, *On the number of inductively minimal geometries*, Theoret. Comput. Sci. **263** (2001), no. 1-2, 31–35, Combinatorics and computer science (Palaiseau, 1997). MR MR1846914 (2002e:05010)
- [4] Stephen P. Humphries and Zane Kun Li, *Counting powers of words in monoids*, European J. Combin. **30** (2009), no. 5, 1297–1308. MR MR2514653
- [5] Byungchan Kim, *On inequalities and linear relations for 7-core partitions*, Discrete Math. **310** (2010), no. 4, 861–868.
- [6] Ken Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and  $q$ -series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR MR2020489 (2005c:11053)
- [7] Kevin T. Phelps, *An enumeration of 1-perfect binary codes*, Australas. J. Combin. **21** (2000), 287–298. MR MR1758278 (2001a:94050)
- [8] Wilhelm Plesken, *Counting with groups and rings*, J. Reine Angew. Math. **334** (1982), 40–68. MR MR667449 (84a:20008)
- [9] A. Stoimenow, *Generating functions, Fibonacci numbers and rational knots*, J. Algebra **310** (2007), no. 2, 491–525. MR MR2308169 (2008a:05018)
- [10] Paul van Wamelen, *Enumerating Motzkin-Rabin geometries*, J. Combin. Des. **15** (2007), no. 3, 179–194. MR MR2311187 (2008b:05013)
- [11] H. A. Verrill, *Sums of squares of binomial coefficients, with applications to Picard-Fuchs equations*, 2004.

# Designs and Configurations

05Bxx

- [1] David Applegate, E. M. Rains, and N. J. A. Sloane, *On asymmetric coverings and covering numbers*, J. Combin. Des. **11** (2003), no. 3, 218–228. MR MR1973254 (2004b:05058)
- [2] Makoto Araya, Masaaki Harada, and Hadi Kharaghani, *Some Hadamard matrices of order 32 and their binary codes*, J. Combin. Des. **12** (2004), no. 2, 142–146. MR MR2036652 (2004m:94092)
- [3] E. F. Assmus, Jr. and J. D. Key, *Translation planes and derivation sets*, J. Geom. **37** (1990), no. 1-2, 3–16. MR MR1041974 (92e:51018a)
- [4] ———, *Hadamard matrices and their designs: A coding-theoretic approach*, Trans. Amer. Math. Soc. **330** (1992), no. 1, 269–293. MR MR1055565 (92f:05024)
- [5] R. A. Bailey, Peter J. Cameron, Peter Dobcsányi, John P. Morgan, and Leonard H. Soicher, *Designs on the web*, Discrete Math. **306** (2006), no. 23, 3014–3027. MR MR2273130 (2007g:05017)
- [6] John Bamberg and Tim Penttila, *A classification of transitive ovoids, spreads, and  $m$ -systems of polar spaces*, Forum Math. **21** (2009), no. 2, 181–216. MR MR2503303
- [7] Eiichi Bannai and Etsuko Bannai, *On Euclidean tight 4-designs*, J. Math. Soc. Japan **58** (2006), no. 3, 775–804. MR MR2254411
- [8] L. M. Batten and J. M. Dover, *Some sets of type  $(m, n)$  in cubic order planes*, Des. Codes Cryptogr. **16** (1999), no. 3, 211–213. MR MR1689577 (2000d:51011)
- [9] Thomas Beth, Christopher Charney, Markus Grassl, Gernot Alber, Aldo Delgado, and Michael Mussinger, *A new class of designs which protect against quantum jumps*, Des. Codes Cryptogr. **29** (2003), no. 1-3, 51–70. MR MR1993156 (2004i:94065)
- [10] Anton Betten, Adalbert Kerber, Reinhard Laue, and Alfred Wassermann, *Simple 8-designs with small parameters*, Des. Codes Cryptogr. **15** (1998), no. 1, 5–27. MR MR1643532 (99g:05019)
- [11] A. Bonnet, E. Rains, and P. Solé, *3-colored 5-designs and  $Z_4$ -codes*, J. Statist. Plann. Inference **86** (2000), no. 2, 349–368. MR MR1768278 (2001g:05021)



- [12] A. Bonnetcaze, P. Solé, and P. Udaya, *Tricolore 3-designs in type III codes*, Discrete Math. **241** (2001), no. 1-3, 129–138. MR MR1861413 (2002m:05031)
- [13] Alexis Bonnetcaze, Bernard Mourrain, and Patrick Solé, *Jacobi polynomials, type II codes, and designs*, Des. Codes Cryptogr. **16** (1999), no. 3, 215–234. MR MR1689581 (2000b:05032)
- [14] Thomas Britz and Carrie G. Rutherford, *Covering radii are not matroid invariants*, Discrete Math. **296** (2005), no. 1, 117–120. MR MR2148485 (2005m:05048)
- [15] Thomas Britz and Keisuke Shiromoto, *Designs from subcode supports of linear codes*, Des. Codes Cryptogr. **46** (2008), no. 2, 175–189. MR MR2368992 (2009a:94040)
- [16] S. Allen Broughton, Robert M. Dirks, Maria T. Slougher, and C. Ryan Vinroot, *Triangular surface tiling groups for low genus*, 2001.
- [17] F. Buekenhout, A. Delandtsheer, and J. Doyen, *Finite linear spaces with flag-transitive groups*, J. Combin. Theory Ser. A **49** (1988), no. 2, 268–293. MR MR964388 (89k:20007)
- [18] A. R. Camina and L. Di Martino, *Block designs on 196 points*, Arch. Math. (Basel) **53** (1989), no. 4, 414–416. MR MR1016008 (90g:05032)
- [19] ———, *The group of automorphisms of a transitive 2-(91, 6, 1) design*, Geom. Dedicata **31** (1989), no. 2, 151–164. MR MR1012437 (91a:20006)
- [20] I. Cardinali, N. Durante, T. Penttila, and R. Trombetti, *Bruen chains over fields of small order*, Discrete Math. **282** (2004), no. 1-3, 245–247. MR MR2059524 (2004m:51008)
- [21] L. L. Carpenter and J. D. Key, *On Hadamard matrices from resolvable Steiner designs*, Proceedings of the Twenty-sixth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1995), vol. 108, 1995, pp. 53–63. MR MR1369276 (96h:05034)
- [22] David B. Chandler and Qing Xiang, *Cyclic relative difference sets and their p-ranks*, Des. Codes Cryptogr. **30** (2003), no. 3, 325–343. MR MR2009282 (2004j:05031)
- [23] Chris Charnes, Martin Rötteler, and Thomas Beth, *Homogeneous bent functions, invariants, and designs*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 139–154. MR MR1919874 (2003h:05043)

- [24] D. Combe, W. D. Palmer, and W. R. Unger, *Bhaskar Rao designs and the alternating group  $A_4$* , Australas. J. Combin. **24** (2001), 275–283. MR MR1852826 (2002f:05027)
- [25] Marston Conder and John McKay, *Markings of the Golay code*, New Zealand J. Math. **25** (1996), no. 2, 133–139. MR MR1421485 (97g:05040)
- [26] Antonio Cossidente and Sam K. J. Vereecke, *Some geometry of the isomorphism  $\text{Sp}(4, q) \cong \text{O}(5, q)$ ,  $q$  even*, J. Geom. **70** (2001), no. 1-2, 28–37. MR MR1825542 (2002g:05043)
- [27] M. R. Darafsheh, A. Iranmanesh, and R. Kahkeshani, *Some designs and codes invariant under the groups  $S_9$  and  $A_8$* , Des. Codes Cryptogr. **51** (2009), no. 2, 211–223. MR MR2480700 (2009k:05193)
- [28] Warwick de Launey and Richard M. Stafford, *On cocyclic weighing matrices and the regular group actions of certain Paley matrices*, Discrete Appl. Math. **102** (2000), no. 1-2, 63–101. MR MR1758337 (2001d:05027)
- [29] U. Dempwolff, *Automorphisms and equivalence of bent functions and of difference sets in elementary abelian 2-groups*, Comm. Algebra **34** (2006), no. 3, 1077–1131. MR MR2208119 (2006m:05035)
- [30] Cunsheng Ding, Zeying Wang, and Qing Xiang, *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in  $\text{PG}(3, 3^{2h+1})$* , J. Combin. Theory Ser. A **114** (2007), no. 5, 867–887. MR MR2333138
- [31] Cunsheng Ding and Jin Yuan, *A family of skew Hadamard difference sets*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1526–1535. MR MR2259075 (2008c:05020)
- [32] G. L. Ebert, *Quasimultiples of geometric designs*, Discrete Math. **284** (2004), no. 1-3, 123–129. MR MR2071902 (2005b:05049)
- [33] Ronald Evans, Henk D. L. Hollmann, Christian Krattenthaler, and Qing Xiang, *Gauss sums, Jacobi sums, and  $p$ -ranks of cyclic difference sets*, J. Combin. Theory Ser. A **87** (1999), no. 1, 74–119. MR MR1698269 (2001b:05038)
- [34] Tao Feng, *Non-abelian skew hadamard difference sets fixed by a prescribed automorphism*, J Combin. Theory Ser. A **To appear** (2009).
- [35] W. Fish, J. D. Key, and E. Mwambene, *Graphs, designs and codes related to the  $n$ -cube*, Discrete Math. **309** (2009), no. 10, 3255–3269. MR MR2526744

- [36] D. L. Flannery, *Cocyclic Hadamard matrices and Hadamard groups are equivalent*, J. Algebra **192** (1997), no. 2, 749–779. MR MR1452686 (98f:20036)
- [37] Anna Fukshansky and Corinna Wiedorn, *C-extensions of the Petersen geometry for  $M_{22}$* , European J. Combin. **20** (1999), no. 3, 233–238. MR MR1687239 (2000f:05089)
- [38] S. Georgiou, I. Kotsireas, and C. Koukouvinos, *Inequivalent Hadamard matrices of order  $2n$  constructed from Hadamard matrices of order  $n$* , J. Combin. Math. Combin. Comput. **63** (2007), 65–79. MR MR2363911 (2008i:05024)
- [39] S. Georgiou and C. Koukouvinos, *Some results on orthogonal designs and Hadamard matrices*, Int. J. Appl. Math. **17** (2005), no. 4, 433–443. MR MR2199768 (2007b:05032)
- [40] Stelios D. Georgiou, *New two-variable full orthogonal designs and related experiments with linear regression models*, Statist. Probab. Lett. **77** (2007), no. 1, 25–31. MR MR2339015
- [41] Claudia Gohlich, Helmut Koch, and Gabriele Nebe, *Block squares*, Math. Nachr. **241** (2002), 73–102. MR MR1912379 (2003f:05013)
- [42] Ken Gray, *On the minimum number of blocks defining a design*, Bull. Austral. Math. Soc. **41** (1990), no. 1, 97–112. MR MR1043970 (91e:05016)
- [43] Masaaki Harada, *On the self-dual  $F_5$ -codes constructed from Hadamard matrices of order 24*, J. Combin. Des. **13** (2005), no. 2, 152–156. MR MR2116198 (2005i:05026)
- [44] ———, *Self-orthogonal  $3$ -(56, 12, 65) designs and extremal doubly-even self-dual codes of length 56*, Des. Codes Cryptogr. **38** (2006), no. 1, 5–16. MR MR2191121 (2006h:94250)
- [45] Masaaki Harada, Clement Lam, and Vladimir D. Tonchev, *Symmetric  $(4, 4)$ -nets and generalized Hadamard matrices over groups of order 4*, Des. Codes Cryptogr. **34** (2005), no. 1, 71–87. MR MR2126578
- [46] Masaaki Harada and Akihiro Munemasa, *A quasi-symmetric  $2$ -(49, 9, 6) design*, J. Combin. Des. **10** (2002), no. 3, 173–179. MR MR1896652 (2003c:05035)
- [47] Masaaki Harada and Vladimir D. Tonchev, *Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms*, Discrete Math. **264** (2003), no. 1-3, 81–90, The 2000 Com<sup>2</sup>MaC Conference on Association Schemes, Codes and Designs (Po-hang). MR MR1972023 (2004f:94099)

- [48] K. J. Horadam, *An introduction to cocyclic generalised Hadamard matrices*, Discrete Appl. Math. **102** (2000), no. 1-2, 115–131, Coding, cryptography and computer security (Lethbridge, AB, 1998). MR MR1758339 (2001i:05043)
- [49] ———, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, 2007. MR MR2265694 (2008d:05036)
- [50] Naoyuki Horiguchi, Hiroyuki Nakasora, and Takehisa Wakabayashi, *On the strongly regular graphs obtained from quasi-symmetric 2-(31, 7, 7) designs*, Bull. Yamagata Univ. Natur. Sci. **16** (2005), no. 1, 1–6. MR MR2127982 (2006c:05146)
- [51] Masakazu Jimbo and Keisuke Shiromoto, *A construction of mutually disjoint Steiner systems from isomorphic Golay codes*, J. Combin. Theory Ser. A **116** (2009), no. 7, 1245–1251. MR MR2527609
- [52] G. A. Kadir and J. D. Key, *The Steiner system  $S(5, 8, 24)$  constructed from dual affine planes*, Proc. Roy. Soc. Edinburgh Sect. A **103** (1986), no. 1-2, 147–160. MR MR858124 (87j:05049)
- [53] Wen-Fong Ke, *On nonisomorphic BIBD with identical parameters*, Combinatorics '90 (Gaeta, 1990), Ann. Discrete Math., vol. 52, North-Holland, Amsterdam, 1992, pp. 337–346. MR MR1195821 (93k:05018)
- [54] J. D. Key, *Extendable Steiner designs*, Geom. Dedicata **41** (1992), no. 2, 201–205. MR MR1153983 (93h:05036)
- [55] ———, *On a class of 1-designs*, European J. Combin. **14** (1993), no. 1, 37–41. MR MR1197474 (93m:05021)
- [56] ———, *Extendable Steiner designs from finite geometries*, J. Statist. Plann. Inference **56** (1996), no. 2, 181–186, Special issue on orthogonal arrays and affine designs, Part II. MR MR1436004 (97j:05020)
- [57] J. D. Key and M. J. de Resmini, *Small sets of even type and codewords*, J. Geom. **61** (1998), no. 1-2, 83–104. MR MR1603821 (98k:51024)
- [58] J. D. Key and K. Mackenzie, *Ovals in the designs  $W(2^m)$* , Ars Combin. **33** (1992), 113–117. MR MR1174835 (93d:05035)

- [59] J. D. Key and K. Mackenzie-Fleming, *Rigidity theorems for a class of affine resolvable designs*, J. Combin. Math. Combin. Comput. **35** (2000), 147–160. MR MR1806994 (2001m:05040)
- [60] J. D. Key, T. P. McDonough, and V. C. Mavron, *Partial permutation decoding for codes from finite planes*, European J. Combin. **26** (2005), no. 5, 665–682. MR MR2127688 (2005k:05056)
- [61] J. D. Key and J. Moorj, *Codes, designs and graphs from the Janko groups  $J_1$  and  $J_2$* , J. Combin. Math. Combin. Comput. **40** (2002), 143–159. MR MR1887973 (2002m:05035)
- [62] J. D. Key and F. D. Shobe, *Some transitive Steiner triple systems of Bagchi and Bagchi*, J. Statist. Plann. Inference **58** (1997), no. 1, 79–86. MR MR1437033 (98i:05020)
- [63] J. D. Key and F. E. Sullivan, *Codes of Steiner triple and quadruple systems*, Des. Codes Cryptogr. **3** (1993), no. 2, 117–125. MR MR1218944 (94e:05050)
- [64] ———, *Steiner triple systems with many affine hyperplanes*, Proceedings of the Twenty-sixth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1995), vol. 107, 1995, pp. 105–112. MR MR1369258
- [65] Michael Kiermaier and Sascha Kurz, *Maximal integral point sets in affine planes over finite fields*, Discrete Math. **309** (2009), no. 13, 4564–4575. MR MR2519195
- [66] Jon-Lark Kim and Vera Pless, *Designs in additive codes over  $\text{GF}(4)$* , Des. Codes Cryptogr. **30** (2003), no. 2, 187–199. MR MR2007210 (2005b:94067)
- [67] Jon-Lark Kim and Patrick Solé, *Skew Hadamard designs and their codes*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 135–145. MR MR2438446
- [68] I. S. Kotsireas and C. Koukouvinos, *Inequivalent hadamard matrices from orthogonal designs*, PASCO '07: Proceedings of the 2007 International Workshop on Parallel Symbolic Computation (New York, NY, USA), ACM, 2007, pp. 95–96.
- [69] Ilias S. Kotsireas and Christos Koukouvinos, *Constructions for Hadamard matrices of Williamson type*, J. Combin. Math. Combin. Comput. **59** (2006), 17–32. MR MR2277340 (2007g:05033)
- [70] ———, *Orthogonal designs via computational algebra*, J. Combin. Des. **14** (2006), no. 5, 351–362. MR MR2245551

- [71] Ilias S. Kotsireas, Christos Koukouvinos, and Jennifer Seberry, *Hadamard ideals and Hadamard matrices with circulant core*, J. Combin. Math. Combin. Comput. **57** (2006), 47–63. MR MR2226682 (2007a:05024)
- [72] ———, *Hadamard ideals and Hadamard matrices with two circulant cores*, European J. Combin. **27** (2006), no. 5, 658–668. MR MR2215425
- [73] C. Koukouvinos and S. Stylianou, *On skew-Hadamard matrices*, Discrete Math. **308** (2008), no. 13, 2723–2731. MR MR2413970
- [74] Christos Koukouvinos and Dimitris E. Simos, *Improving the lower bounds on inequivalent Hadamard matrices through orthogonal designs and meta-programming techniques*, Applied Numerical Mathematics **To appear** (2009).
- [75] Wolfgang Lempken, *Two new symmetric 2-(144, 66, 30) designs*.
- [76] Keith E. Mellinger, *Designs, Geometry, and a Golfer’s Dilemma*, Math. Mag. **77** (2004), no. 4, 275–282. MR MR1573761
- [77] Jamshid Moori and B. G. Rodrigues, *Some designs and codes invariant under the simple group  $\text{Co}_2$* , J. Algebra **316** (2007), no. 2, 649–661. MR MR2358607
- [78] Akihiro Munemasa and Vladimir D. Tonchev, *A new quasi-symmetric 2-(56, 16, 6) design obtained from codes*, Discrete Math. **284** (2004), no. 1-3, 231–234. MR MR2071915 (2005b:05027)
- [79] Werner Nickel, Alice C. Niemeyer, Christine M. O’Keefe, Tim Penttila, and Cheryl E. Praeger, *The block-transitive, point-imprimitive 2-(729, 8, 1) designs*, Appl. Algebra Engrg. Comm. Comput. **3** (1992), no. 1, 47–61. MR MR1325745 (96j:05024)
- [80] Christopher Parker, Edward Spence, and Vladimir D. Tonchev, *Designs with the symmetric difference property on 64 points and their groups*, J. Combin. Theory Ser. A **67** (1994), no. 1, 23–43. MR MR1280597 (95d:05021)
- [81] Christopher Parker and Vladimir D. Tonchev, *Linear codes and doubly transitive symmetric designs*, Linear Algebra Appl. **226/228** (1995), 237–246. MR MR1344564 (96e:05021)
- [82] E. M. Rains, N. J. A. Sloane, and John Stufken, *The lattice of  $N$ -run orthogonal arrays*, J. Statist. Plann. Inference **102** (2002), no. 2, 477–500, Silver jubilee issue. MR MR1897221 (2003c:62138)

- [83] Colin Ramsay, *Trades and defining sets: Theoretical and computational results*, Ph.D. thesis, University of Queensland, 1998, pp. 1–223.
- [84] B. G. Rodrigues, *Self-orthogonal designs and codes from the symplectic groups  $S_4(3)$  and  $S_4(4)$* , Discrete Math. **308** (2008), no. 10, 1941–1950. MR MR2394462 (2009a:05022)
- [85] Nagwa Kamal Ahmed Rostom, *On the  $p$ -rank of  $t$ -designs*, MSc Thesis, University of Birmingham, 1985.
- [86] Chekad Sarami and Vladimir D. Tonchev, *Cyclic quasi-symmetric designs and self-orthogonal codes of length 63*, J. Statist. Plann. Inference **138** (2008), no. 1, 80–85. MR MR2369615 (2009b:05039)
- [87] Bernd Schmalz,  *$t$ -Designs zu vorgegebener Automorphismengruppe*, Bayreuth. Math. Schr. (1992), no. 41, 164, Dissertation, Universität Bayreuth, Bayreuth, 1992. MR MR1166044 (93f:05024)
- [88] Michel Seville, *On a result of Cameron and Praeger on block-transitive point-imprimitive  $t$ -designs*, Algebraic Combinatorics and Applications (Gößweinstein, 1999), Springer, Berlin, 2001, pp. 316–323. MR MR1851959 (2002j:05022)
- [89] Martin J. Sharry, *Partitioning sets of quintuples into designs*, J. Combin. Math. Combin. Comput. **6** (1989), 67–103. MR MR1025009 (90j:05034)
- [90] Junichi Shigezumi, *On 3-lattices and spherical designs*, 2008.
- [91] Pawel Wocjan, *Efficient decoupling schemes with bounded controls based on Eulerian orthogonal arrays*, Phy. Rev. A. **73** (2006), no. 6, 7.

# Graph Theory

05Cxx

- [1] David Abelson, Seok-Hee Hong, and D. E. Taylor, *Geometric automorphism groups of graphs*, Discrete Appl. Math. **155** (2007), no. 17, 2211–2226. MR MR2360651
- [2] David Abelson, Seok-Hee Hong, and Donald E. Taylor, *A group-theoretic method for drawing graphs symmetrically*, Graph Drawing, Lecture Notes in Comput. Sci., vol. 2528, Springer, Berlin, 2002, pp. 86–97. MR MR2063414
- [3] R. D. Baker, G. L. Ebert, J. Hemmeter, and A. Woldar, *Maximal cliques in the Paley graph of square order*, J. Statist. Plann. Inference **56** (1996), no. 1, 33–38, Special issue on orthogonal arrays and affine designs, Part I. MR MR1435518 (98a:05084)
- [4] John Bamberg, Geoffrey Pearce, and Cheryl E. Praeger, *Transitive decompositions of graph products: Rank 3 grid type*, J. Group Theory **11** (2008), no. 2, 185–228. MR MR2396959
- [5] Eiichi Bannai, Osamu Shimabukuro, and Hajime Tanaka, *Finite analogues of non-Euclidean spaces and Ramanujan graphs*, European J. Combin. **25** (2004), no. 2, 243–259. MR MR2070545 (2005g:05066)
- [6] ———, *Finite Euclidean graphs and Ramanujan graphs*, Discrete Math. **309** (2009), no. 20, 6126–6134. MR MR2552647
- [7] Wayne Barrett, Jason Grout, and Raphael Loewy, *The minimum rank problem over the finite field of order 2: minimum rank 3*, Linear Algebra and its Applications **430** (2009), no. 4, 890 – 923.
- [8] C. Bates, D. Bundy, Sarah B. Perkins, and P. Rowley, *Commuting involution graphs for symmetric groups*, J. Algebra **266** (2003), no. 1, 133–153. MR MR1994533 (2004h:20004)
- [9] N. L. Biggs, *Presentations for cubic graphs*, Computational Group Theory (Durham, 1982), Academic Press, London, 1984, pp. 57–63. MR MR760649 (86b:05037)
- [10] Norman Biggs, *Constructions for cubic graphs with large girth*, Electron. J. Combin. **5** (1998), Article 1, 25 pp. (electronic). MR MR1661181 (99j:05097)



- [11] Mireille Boutin and Gregor Kemper, *Lossless representation of graphs using distributions*, 2007.
- [12] John M. Boyer and Wendy J. Myrvold, *On the cutting edge: Simplified  $O(n)$  planarity by edge addition*, J. Graph Algorithms Appl. **8** (2004), no. 3, 241–273 (electronic). MR MR2166815
- [13] John Bray, Christopher Parker, and Peter Rowley, *Cayley type graphs and cubic graphs of large girth*, Discrete Math. **214** (2000), no. 1-3, 113–121. MR MR1743630 (2000j:05055)
- [14] Andries E. Brouwer, Naoyuki Horiguchi, Masaaki Kitazume, and Hiroyuki Nakasora, *A construction of the sporadic Suzuki graph from  $U_3(4)$* , J. Combin. Theory Ser. A **116** (2009), no. 5, 1056–1062. MR MR2522419
- [15] Pierre Cartier, *Combinatorics of trees*, Surveys in modern mathematics, London Math. Soc. Lecture Note Ser., vol. 321, Cambridge Univ. Press, Cambridge, 2005, pp. 274–282. MR MR2166933
- [16] Marston Conder, *A note on Cayley graphs*, J. Combin. Theory Ser. B **40** (1986), no. 3, 362–368. MR MR843000 (87g:05113)
- [17] ———, *Groups of minimal genus including  $C_2$  extensions of  $\text{PSL}(2, q)$  for certain  $q$* , Quart. J. Math. Oxford Ser. (2) **38** (1987), no. 152, 449–460. MR MR916227 (89a:20043)
- [18] ———, *A new 5-arc-transitive cubic graph*, J. Graph Theory **11** (1987), no. 3, 303–307. MR MR902707 (88f:05054)
- [19] ———, *Maximal automorphism groups of symmetric Riemann surfaces with small genus*, J. Algebra **114** (1988), no. 1, 16–28. MR MR931896 (89c:20049)
- [20] ———, *Constructing symmetric graphs*, Theta **3** (1989), 11–16.
- [21] ———, *An infinite family of 4-arc-transitive cubic graphs each with girth 12*, Bull. London Math. Soc. **21** (1989), no. 4, 375–380. MR MR998635 (90d:05115)
- [22] ———, *Experimental algebra*, Math. Chronicle **20** (1991), 1–11. MR MR1137869 (92k:20007)

- [23] ———, *Group actions on the cubic tree*, J. Algebraic Combin. **1** (1992), no. 3, 209–218. MR MR1194075 (94b:20034)
- [24] ———, *Regular maps with small parameters*, J. Austral. Math. Soc. Ser. A **57** (1994), no. 1, 103–112. MR MR1279289 (95h:05087)
- [25] ———, *Group actions on graphs, maps and surfaces with maximum symmetry*, Groups St. Andrews 2001 in Oxford. Vol. I, London Math. Soc. Lecture Note Ser., vol. 304, Cambridge Univ. Press, Cambridge, 2003, pp. 63–91. MR MR2051519 (2004m:20005)
- [26] Marston Conder, *Genus spectra for symmetric embeddings of graphs on surfaces*, Electronic Notes in Discrete Mathematics **31** (2008), 27 – 31.
- [27] Marston Conder, *On symmetries of Cayley graphs and the graphs underlying regular maps*, J. Algebra **321** (2009), no. 11, 3112–3127. MR MR2510042
- [28] Marston Conder and Peter Dobcsányi, *Determination of all regular maps of small genus*, J. Combin. Theory Ser. B **81** (2001), no. 2, 224–242. MR MR1814906 (2002f:05088)
- [29] ———, *Trivalent symmetric graphs on up to 768 vertices*, J. Combin. Math. Combin. Comput. **40** (2002), 41–63. MR MR1887966 (2002m:05105)
- [30] Marston Conder and Brent Everitt, *Regular maps on non-orientable surfaces*, Geom. Dedicata **56** (1995), no. 2, 209–219. MR MR1338960 (96g:05046)
- [31] Marston Conder, Robert Jajcay, and Thomas Tucker, *Regular Cayley maps for finite abelian groups*, J. Algebraic Combin. **25** (2007), no. 3, 259–283. MR MR2317333 (2008d:05069)
- [32] Marston Conder and Cai Heng Li, *On isomorphisms of finite Cayley graphs*, European J. Combin. **19** (1998), no. 8, 911–919. MR MR1657923 (99i:05096)
- [33] Marston Conder and Peter Lorimer, *Automorphism groups of symmetric graphs of valency 3*, J. Combin. Theory Ser. B **47** (1989), no. 1, 60–72. MR MR1007714 (90g:05097)
- [34] Marston Conder, Peter Lorimer, and Cheryl Praeger, *Constructions for arc-transitive digraphs*, J. Austral. Math. Soc. Ser. A **59** (1995), no. 1, 61–80. MR MR1336452 (96i:05095)

- [35] Marston Conder, Aleksander Malnič, Dragan Marušič, Tomaž Pisanski, and Primož Potočnik, *The edge-transitive but not vertex-transitive cubic graph on 112 vertices*, J. Graph Theory **50** (2005), no. 1, 25–42. MR MR2157536 (2006c:05071)
- [36] Marston Conder, Aleksander Malnič, Dragan Marušič, and Primož Potočnik, *A census of semisymmetric cubic graphs on up to 768 vertices*, J. Algebraic Combin. **23** (2006), no. 3, 255–294. MR MR2228929 (2007g:05077)
- [37] Marston Conder and Dragan Marušič, *A tetravalent half-arc-transitive graph with non-abelian vertex stabilizer*, J. Combin. Theory Ser. B **88** (2003), no. 1, 67–76. MR MR1973260 (2004d:05086)
- [38] Marston Conder, Margaret Morton, and Cheryl E. Praeger, *Partition graphs for finite symmetric groups*, J. Graph Theory **25** (1997), no. 2, 107–117. MR MR1448847 (98g:05069)
- [39] ———, *Two-arc closed subsets of graphs*, J. Graph Theory **42** (2003), no. 4, 350–364. MR MR1963107 (2004a:05133)
- [40] Marston Conder and Roman Nedela, *Symmetric cubic graphs of small girth*, J. Combin. Theory Ser. B **97** (2007), no. 5, 757–768. MR MR2344138
- [41] ———, *A refined classification of symmetric cubic graphs*, J. Algebra **322** (2009), no. 3, 722–740. MR MR2531219
- [42] Marston Conder and Roman Nedela, *A refined classification of symmetric cubic graphs*, J. Algebra **322** (2009), no. 1, 722–740.
- [43] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular hypermaps over projective linear groups*, J. Aust. Math. Soc. **85** (2008).
- [44] Marston Conder, Jozef Širáň, and Tom Tucker, *The genera, reflexivity and simplicity of regular maps*, J. Eur. Math. Soc. (JEMS) **To appear**.
- [45] Marston Conder and Cameron G. Walker, *The infinitude of 7-arc-transitive graphs*, J. Algebra **208** (1998), no. 2, 619–629. MR MR1655469 (99j:05089)
- [46] Marston Conder and Steve Wilson, *Inner reflectors and non-orientable regular maps*, Discrete Math. **307** (2007), no. 3-5, 367–372. MR MR2287477

- [47] Maria Cristeta Cuaresma, Michael Giudici, and Cheryl E. Praeger, *Homogeneous factorisations of Johnson graphs*, Des. Codes Cryptogr. **46** (2008), no. 3, 303–327. MR MR2372841 (2008j:05163)
- [48] Italo J. Dejter, *C-homogeneous graphs via ordered pencils*, 2007.
- [49] Italo J. Dejter, *On Clique Turan graph-homogeneity*, 2007.
- [50] Italo J. Dejter, *On a  $\{K_4, K_{2,2,2}\}$ -ultrahomogeneous graph.*, Australas. J. Comb. **44** (2009), 63–75.
- [51] Italo J. Dejter, *A construction based on the Biggs-Smith graph*, 2010.
- [52] A. Delgado and R. Weiss, *On certain coverings of generalized polygons*, Bull. London Math. Soc. **21** (1989), no. 3, 235–242. MR MR986364 (90b:20004)
- [53] Alice Devillers and Michael Giudici, *Involution graphs where the product of two adjacent vertices has order three*, J. Aust. Math. Soc. **85** (2008), no. 3, 305–322.
- [54] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *A remarkable Mathieu graph tower*.
- [55] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *Primitive decompositions of Johnson graphs*, J. Combin. Theory Ser. A **115** (2008), no. 6, 925–966. MR MR2423342
- [56] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *An infinite family of biquasiprimitive 2-arc transitive cubic graphs*, 2009, pp. 1–19.
- [57] ———, *Locally s-distance transitive graphs*, 2010.
- [58] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *Some graphs related to the small Mathieu groups*, European J. Combin. **31** (2010), no. 1, 336–348. MR MR2552613
- [59] Michael J. Dinneen and Paul R. Hafner, *New results for the degree/diameter problem*, Networks **24** (1994), no. 7, 359–367. MR MR1294788 (95h:05141)
- [60] Edward Dobson and Dragan Marušič, *An unusual decomposition of a complete 7-partite graph of order 28*, Discrete Math. **308** (2008), no. 20, 4595–4598. MR MR2438164

- [61] Xin Gui Fang, George Havas, and Cheryl E. Praeger, *On the automorphism groups of quasiprimitive almost simple graphs*, J. Algebra **222** (1999), no. 1, 271–283. MR MR1728159 (2000j:05056)
- [62] Xin Gui Fang, George Havas, and Jie Wang, *Automorphism groups of certain non-quasiprimitive almost simple graphs*, Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 267–274. MR MR1676623 (2000h:05104)
- [63] Yan-Quan Feng, Klavdija Kutnar, Aleksander Malnič, and Dragan Marušič, *On 2-fold covers of graphs*, J. Combin. Theory Ser. B **98** (2008), no. 2, 324–341. MR MR2389602 (2009d:05104)
- [64] Yan-Quan Feng, Jin Ho Kwak, and Chuixiang Zhou, *Constructing even radius tightly attached half-arc-transitive graphs of valency four*, J. Algebraic Combin. **26** (2007), no. 4, 431–451. MR MR2341859
- [65] Louis Ferré and Bertrand Jouve, *Vertex partitioning of a class of digraphs*, Math. Sci. Hum. (2002), no. 158, 59–77. MR MR1952409 (2003m:05089)
- [66] Carla Fiori and Beatrice Ruini, *Infinite classes of dihedral snarks*, Mediterr. J. Math. **5** (2008), no. 2, 199–210. MR MR2427394
- [67] W. Fish, J. D. Key, and E. Mwambene, *Graphs, designs and codes related to the  $n$ -cube*, Discrete Math. **309** (2009), no. 10, 3255–3269. MR MR2526744
- [68] Michael Giudici, Cai Heng Li, Primož Potočnik, and Cheryl E. Praeger, *Homogeneous factorisations of complete multipartite graphs*, Discrete Math. **307** (2007), no. 3-5, 415–431. MR MR2287483
- [69] Michael Giudici and Aedan Pope, *The diameters of commuting graphs of linear groups and matrix rings over the integers modulo  $m$* , 2010.
- [70] H. H. Glover, K. Kutnar, and Dragan Marušič, *Hamiltonian cycles in cubic Cayley graphs: The  $j2, 4k, 3j$  case*, J. Algebraic Combin. **To appear** (2009).
- [71] Jason Grout, *Ultraconnected and critical graphs*, Master of science, Brigham Young University, 2003.

- [72] Paul R. Hafner, *Large Cayley graphs and digraphs with small degree and diameter*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 291–302. MR MR1344938 (96e:05070)
- [73] ———, *Geometric realisation of the graphs of McKay-Miller-širáň*, J. Combin. Theory Ser. B **90** (2004), no. 2, 223–232. MR MR2034028 (2005a:05152)
- [74] ———, *On the graphs of Hoffman-Singleton and Higman-Sims*, Electron. J. Combin. **11** (2004), no. 1, Research Paper 77, 33 pp. (electronic). MR MR2114181 (2005k:05167)
- [75] Stephen P. Humphries, *Quotients of Coxeter complexes, fundamental groupoids and regular graphs*, Math. Z. **217** (1994), no. 2, 247–273. MR MR1296396 (95i:20059)
- [76] A. A. Ivanov and Cheryl E. Praeger, *On finite affine 2-arc transitive graphs*, European J. Combin. **14** (1993), no. 5, 421–444, Algebraic combinatorics (Vladimir, 1991). MR MR1241910 (94k:05089)
- [77] Robert E. Jamison and Gretchen L. Matthews, *Distance  $k$  colorings of Hamming graphs*, Proceedings of the Thirty-Seventh Southeastern International Conference on Combinatorics, Graph Theory and Computing, vol. 183, 2006, pp. 193–202. MR MR2311479
- [78] Peter Keevash and Benny Sudakov, *Packing triangles in a graph and its complement*, J. Graph Theory **47** (2004), no. 3, 203–216. MR MR2089464 (2005g:05119)
- [79] István Kovács, Klavdija Kutnar, and János Ruff, *Rose window graphs underlying rotary maps*, Discrete Math. **310** (2010), no. 12, 1802–1811. MR 2610284
- [80] István Kovács, Aleksander Malnič, Dragan Marušič, and Štefko Miklavič, *One-matching bi-Cayley graphs over abelian groups*, European J. Combin. **30** (2009), no. 2, 602–616. MR MR2489254
- [81] K. Kutnar, Aleksander Malnič, Dragan Marušič, and Štefko Miklavič, *The strongly distance-balanced property of the generalized Petersen graphs*, Ars Math. Contemp. **2** (2009), no. 1, 41–47.
- [82] Klavdija Kutnar, Aleksander Malnič, Dragan Marušič, and Štefko Miklavič, *Distance-balanced graphs: Symmetry conditions*, Discrete Math. **306** (2006), no. 16, 1881–1894. MR MR2251569

- [83] Klavdija Kutnar and Dragan Marušič, *Hamiltonicity of vertex-transitive graphs of order  $4p$* , European J. Combin. **29** (2008), no. 2, 423–438. MR MR2388379 (2009a:05116)
- [84] ———, *A complete classification of cubic symmetric graphs of girth 6*, J. Combin. Theory Ser. B **99** (2009), no. 1, 162–184. MR MR2467824
- [85] Klavdija Kutnar and Primož Šparl, *Hamilton paths and cycles in vertex-transitive graphs of order  $6p$* , Discrete Math. **309** (2009), no. 17, 5444–5460. MR MR2548563
- [86] Felix Lazebnik and Raymond Viglione, *An infinite series of regular edge- but not vertex-transitive graphs*, J. Graph Theory **41** (2002), no. 4, 249–258. MR MR1936942 (2003i:05066)
- [87] Cai Heng Li, Tian Khoon Lim, and Cheryl E. Praeger, *Homogeneous factorisations of complete graphs with edge-transitive factors*, J. Algebraic Combin. **29** (2009), no. 1, 107–132. MR MR2470118
- [88] Paulette Lieby, *Colouring planar graphs*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 315–330. MR MR2278934
- [89] Tian Khoon Lim, *Edge-transitive homogeneous factorisations of complete graphs*, 2004.
- [90] Tian Khoon Lim, *Arc-transitive homogeneous factorizations and affine planes*, J. Combin. Des. **14** (2006), no. 4, 290–300. MR MR2229880 (2007c:05153)
- [91] Tian Khoon Lim and Cheryl E. Praeger, *On generalized Paley graphs and their automorphism groups*, Michigan Math. J. **58** (2009), no. 1, 293–308. MR MR2526089
- [92] Peter Lorimer, *The construction of some trivalent symmetric graphs*, Ars Combin. **26** (1988), 107–114. MR MR982112 (90c:05107)
- [93] ———, *The construction of Tutte’s 8-cage and the Conder graph*, J. Graph Theory **13** (1989), no. 5, 553–557. MR MR1016275 (90h:05099)
- [94] ———, *Embeddings of symmetric graphs in surfaces*, Australas. J. Combin. **3** (1991), 31–54. MR MR1122216 (92g:05082)

- [95] Marko Lovrečić Saražin, Walter Pacco, and Andrea Previtali, *Generalizing the generalized Petersen graphs*, Discrete Math. **307** (2007), no. 3-5, 534–543. MR MR2287493
- [96] Aleksander Malnič, Dragan Marušič, Štefko Miklavič, and Primož Potočnik, *Semisymmetric elementary abelian covers of the Möbius-Kantor graph*, Discrete Math. **307** (2007), no. 17-18, 2156–2175. MR MR2340598 (2008g:05097)
- [97] Aleksander Malnič, Dragan Marušič, and Primož Potočnik, *Elementary abelian covers of graphs*, J. Algebraic Combin. **20** (2004), no. 1, 71–97. MR MR2104822 (2005g:05070)
- [98] ———, *On cubic graphs admitting an edge-transitive solvable group*, J. Algebraic Combin. **20** (2004), no. 1, 99–113. MR MR2104823 (2005h:05097)
- [99] Aleksander Malnič, Dragan Marušič, and Primož Šparl, *On strongly regular bicirculants*, European J. Combin. **28** (2007), no. 3, 891–900. MR MR2300769
- [100] Aleksander Malnič and Primož Potočnik, *Invariant subspaces, duality, and covers of the Petersen graph*, European J. Combin. **27** (2006), no. 6, 971–989. MR MR2226431 (2007b:05172)
- [101] Dragan Marušič, *On 2-arc-transitivity of Cayley graphs*, J. Combin. Theory Ser. B **87** (2003), no. 1, 162–196. MR MR1967887 (2004a:05064)
- [102] Dragan Marušič and Primož Potočnik, *Bridging semisymmetric and half-arc-transitive actions on graphs*, European J. Combin. **23** (2002), no. 6, 719–732. MR MR1924793 (2004f:05079)
- [103] Margaret Morton, *A note on arc-transitive circulants*, Bull. Inst. Combin. Appl. **23** (1998), 63–68. MR MR1621756 (99d:05075)
- [104] Margaret J. Morton, *Corrigendum: “Classification of 4- and 5-arc-transitive cubic graphs of small girth” [J. Austral. Math. Soc. Ser. A **50** (1991), no. 1, 138–149; MR1094065 (92e:05053)]*, J. Austral. Math. Soc. Ser. A **52** (1992), no. 3, 419–420. MR MR1151296
- [105] Hiroshi Nozaki, *Geometrical approach to Seidel’s switching for strongly regular graphs*, 2009.
- [106] Ju-Mok Oh, *Arc-transitive elementary abelian covers of the Pappus graph*, Discrete Math. **309** (2009), no. 23-24, 6590–6611. MR MR2558624



- [107] ———, *A classification of cubic  $s$ -regular graphs of order  $14p$* , Discrete Math. **309** (2009), no. 9, 2721–2726. MR MR2523779
- [108] ———, *A classification of cubic  $s$ -regular graphs of order  $16p$* , Discrete Math. **309** (2009), no. 10, 3150–3155. MR MR2526732
- [109] Alen Orbanić, *Parallel-product decomposition of edge-transitive maps*, 2005.
- [110] Michael E. O’Sullivan, *Algebraic construction of sparse matrices with large girth*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 718–727. MR MR2236186
- [111] C. W. Parker, *Semisymmetric cubic graphs of twice odd order*, European J. Combin. **28** (2007), no. 2, 572–591. MR MR2287455
- [112] Christopher Parker and Peter Rowley,  *$\Omega$ -covers of graphs*, Bull. London Math. Soc. **32** (2000), no. 6, 658–662. MR MR1781576 (2001g:05083)
- [113] ———, *Subgroup-chain graphs*, Graphs Combin. **19** (2003), no. 4, 537–545. MR MR2031009 (2004h:05112)
- [114] Manley Perkel and Cheryl E. Praeger, *Polygonal graphs: New families and an approach to their analysis*, Proceedings of the Twenty-eighth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1997), vol. 124, 1997, pp. 161–173. MR MR1605105 (98i:05140)
- [115] Manley Perkel, Cheryl E. Praeger, and Richard Weiss, *On narrow hexagonal graphs with a 3-homogeneous suborbit*, J. Algebraic Combin. **13** (2001), no. 3, 257–273. MR MR1836904 (2002m:05109)
- [116] Adolfo Piperno, *Search space contraction in canonical labeling of graphs (preliminary version)*, 2008.
- [117] Primož Potočnik, *A list of 4-valent 2-arc-transitive graphs and finite faithful amalgams of index  $(4, 2)$* , European J. Combin. **30** (2009), no. 5, 1323–1336. MR MR2514656
- [118] Cheryl E. Praeger and Leonard H. Soicher, *Low Rank Representations and Graphs for Sporadic Groups*, Australian Mathematical Society Lecture Series, vol. 8, Cambridge University Press, Cambridge, 1997. MR MR1430574 (97m:20006)

- [119] Gordon F. Royle and Cheryl E. Praeger, *Constructing the vertex-transitive graphs of order 24*, J. Symbolic Comput. **8** (1989), no. 4, 309–326. MR MR1021609 (91a:68216)
- [120] Stephen T. Schibell and Richard M. Stafford, *Processor interconnection networks from Cayley graphs*, Discrete Appl. Math. **40** (1992), no. 3, 333–357. MR MR1197007 (94a:68005)
- [121] Yin Tan, Alexander Pott, and Tao Feng, *Strongly regular graphs associated with ternary bent functions*, Journal of Combinatorial Theory, Series A **117** (2010), no. 6, 668–682.
- [122] Nicolas M. Thiéry, *Algebraic invariants of graphs; A study based on computer exploration*, SIGSAM Bulletin **34** (2000), no. 3, 9–20.
- [123] V. A. Ustimenko and A. J. Woldar, *An improvement on the Erdős bound for graphs of girth 16*, Second International Conference on Algebra (Barnaul, 1991), Contemp. Math., vol. 184, Amer. Math. Soc., Providence, RI, 1995, pp. 419–425. MR MR1332307 (96c:05102)
- [124] John van Bon and Arjeh M. Cohen, *Linear groups and distance-transitive graphs*, European J. Combin. **10** (1989), no. 5, 399–411. MR MR1014547 (90h:20006)
- [125] John van Bon, Arjeh M. Cohen, and Hans Cuypers, *Graphs related to Held’s simple group*, J. Algebra **123** (1989), no. 1, 6–26. MR MR1000473 (90h:20019)
- [126] Libero Verardi, *Matrices, graphs and equivalence relations*, Ann. Mat. Pura Appl. (4) **180** (2002), no. 4, 413–428. MR MR1877625 (2003a:05104)
- [127] Xiuyun Wang and Yan-Quan Feng, *Hexavalent half-arc-transitive graphs of order  $4p$* , European J. Combin. **30** (2009), no. 5, 1263–1270. MR MR2514648
- [128] Yan Wang, Xin Gui Fang, and D. F. Hsu, *On the edge-forwarding indices of Frobenius graphs*, Acta Math. Sin. (Engl. Ser.) **22** (2006), no. 6, 1735–1744. MR MR2262432
- [129] Richard Weiss, *Presentations for  $(G, s)$ -transitive graphs of small valency*, Math. Proc. Cambridge Philos. Soc. **101** (1987), no. 1, 7–20. MR MR877697 (88c:05063)
- [130] Doug Wiedemann and Michael Zieve, *Equivalence of sparse circulants: The bipartite Adam problem*, 2007.

- [131] Andrew J. Woldar and Vasiliy A. Ustimenko, *An application of group theory to extremal graph theory*, Group Theory (Granville, OH, 1992), World Sci. Publishing, River Edge, NJ, 1993, pp. 293–298. MR MR1348910 (96e:05091)
- [132] Cui Zhang, Jin-Xin Zhou, and Yan-Quan Feng, *Automorphisms of cubic Cayley graphs of order  $2pq$* , Discrete Math. **309** (2009), no. 9, 2687–2695. MR MR2523776
- [133] Jin-Xin Zhou, *Tetravalent  $s$ -transitive graphs of order  $4p$* , Discrete Math. **309** (2009), no. 20, 6081–6086. MR MR2552643
- [134] Jin-Xin Zhou and Yan-Quan Feng, *Tetravalent one-regular graphs of order  $2pq$* , J. Algebraic Combin. **29** (2009), no. 4, 457–471. MR MR2506717
- [135] Jin-Xin Zhou and Yan-Quan Feng, *Cubic vertex-transitive graphs of order  $2pq$* , J. of Graph Theory **65** (2010), no. 4, 263–350.
- [136] Jin-Xin Zhou and Yan-Quan Feng, *Tetravalent  $s$ -transitive graphs of order twice a prime power*, J. Aust. Math. Soc. **88** (2010), no. 2, 277–288.

# Extremal Combinatorics

05Dxx

- [1] Leonid Brailovsky, Dmitrii V. Pasechnik, and Cheryl E. Praeger, *Classification of 2-quasi-invariant subsets*, *Ars Combin.* **42** (1996), 65–76. MR MR1386928 (97a:05204)

# Algebraic Combinatorics

05Exx

- [1] Christine Bachoc, *Harmonic weight enumerators of nonbinary codes and MacWilliams identities*, Codes and Association Schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 1–23. MR MR1816384 (2002b:94024)
- [2] Andries E. Brouwer, Naoyuki Horiguchi, Masaaki Kitazume, and Hiroyuki Nakasora, *A construction of the sporadic Suzuki graph from  $U_3(4)$* , J. Combin. Theory Ser. A **116** (2009), no. 5, 1056–1062. MR MR2522419
- [3] J. Buhler and Z. Reichstein, *Symmetric functions and the phase problem in crystallography*, Trans. Amer. Math. Soc. **357** (2005), no. 6, 2353–2377 (electronic). MR MR2140442
- [4] Marston Conder, *Group actions on graphs, maps and surfaces with maximum symmetry*, Groups St. Andrews 2001 in Oxford. Vol. I, London Math. Soc. Lecture Note Ser., vol. 304, Cambridge Univ. Press, Cambridge, 2003, pp. 63–91. MR MR2051519 (2004m:20005)
- [5] M. R. Darafsheh, A. Iranmanesh, and R. Kahkeshani, *Some designs and codes invariant under the groups  $S_9$  and  $A_8$* , Des. Codes Cryptogr. **51** (2009), no. 2, 211–223. MR MR2480700 (2009k:05193)
- [6] Paul-Olivier Dehaye, *Joint moments of derivatives of characteristic polynomials*, Algebra Number Theory **2** (2008), no. 1, 31–68. MR MR2377362 (2009a:15075)
- [7] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *A remarkable Mathieu graph tower*.
- [8] Steven T. Dougherty, Jon-Lark Kim, and Patrick Solé, *Double circulant codes from two class association schemes*, Adv. Math. Commun. **1** (2007), no. 1, 45–64. MR MR2262767
- [9] Yan-Quan Feng, Jin Ho Kwak, and Chuixiang Zhou, *Constructing even radius tightly attached half-arc-transitive graphs of valency four*, J. Algebraic Combin. **26** (2007), no. 4, 431–451. MR MR2341859

- [10] Anna Fukshansky and Corinna Wiedorn, *C-extensions of the Petersen geometry for  $M_{22}$* , European J. Combin. **20** (1999), no. 3, 233–238. MR MR1687239 (2000f:05089)
- [11] George Havas and Edmund F. Robertson, *Two groups which act on cubic graphs*, Computational Group Theory (Durham, 1982), Academic Press, London, 1984, pp. 65–68. MR MR760650 (86b:05038)
- [12] Naoyuki Horiguchi, Masaaki Kitazume, and Hiroyuki Nakasora, *The Hall-Janko graph and the Witt system  $W_{10}$* , European J. Combin. **29** (2008), no. 1, 1–8. MR MR2368609 (2008j:05369)
- [13] Naoyuki Horiguchi, Hiroyuki Nakasora, and Takehisa Wakabayashi, *On the strongly regular graphs obtained from quasi-symmetric 2-(31, 7, 7) designs*, Bull. Yamagata Univ. Natur. Sci. **16** (2005), no. 1, 1–6. MR MR2127982 (2006c:05146)
- [14] M. Kasatani, T. Miwa, A. N. Sergeev, and A. P. Veselov, *Coincident root loci and Jack and Macdonald polynomials for special values of the parameters*, Jack, Hall-Littlewood and Macdonald Polynomials, Contemp. Math., vol. 417, Amer. Math. Soc., Providence, RI, 2006, pp. 207–225. MR MR2284129
- [15] J. D. Key and J. Moori, *Codes, designs and graphs from the Janko groups  $J_1$  and  $J_2$* , J. Combin. Math. Combin. Comput. **40** (2002), 143–159. MR MR1887973 (2002m:05035)
- [16] J. D. Key, J. Moori, and B. G. Rodrigues, *On some designs and codes from primitive representations of some finite simple groups*, J. Combin. Math. Combin. Comput. **45** (2003), 3–19. MR MR1982631 (2004m:94094)
- [17] M. (ed.) Klin, G.A. (ed.) Jones, A. (ed.) Jurisic, M. (ed.) Muzychuk, and I. (ed.) Ponomarenko, *Algorithmic algebraic combinatorics and gröbner bases*, Springer, Berlin, 2009.
- [18] Klavdija Kutnar, Dragan Marušič, Štefko Miklavič, and Primož Šparl, *Strongly regular tri-Cayley graphs*, European J. Combin. **30** (2009), no. 4, 822–832. MR MR2504641
- [19] Dimitri Leemans, *Locally  $s$ -arc-transitive graphs related to sporadic simple groups*, J. Algebra **322** (2009), no. 3, 882–892. MR MR2531226
- [20] Cai Heng Li, Tian Khoon Lim, and Cheryl E. Praeger, *Homogeneous factorisations of complete graphs with edge-transitive factors*, J. Algebraic Combin. **29** (2009), no. 1, 107–132. MR MR2470118

- [21] Jamshid Moori and B. G. Rodrigues, *A self-orthogonal doubly even code invariant under  $McL : 2$* , J. Combin. Theory Ser. A **110** (2005), no. 1, 53–69. MR MR2128966 (2006a:05174)
- [22] Hiroshi Nozaki, *Geometrical approach to Seidel’s switching for strongly regular graphs*, 2009.
- [23] Ju-Mok Oh, *Arc-transitive elementary abelian covers of the Pappus graph*, Discrete Math. **309** (2009), no. 23-24, 6590–6611. MR MR2558624
- [24] Patric R. J. Östergård, *Classifying subspaces of Hamming spaces*, Des. Codes Cryptogr. **27** (2002), no. 3, 297–305. MR MR1928445 (2003i:94060)
- [25] Christopher Parker, Edward Spence, and Vladimir D. Tonchev, *Designs with the symmetric difference property on 64 points and their groups*, J. Combin. Theory Ser. A **67** (1994), no. 1, 23–43. MR MR1280597 (95d:05021)
- [26] Geoffrey Pearce, *Examples of rank 3 product action transitive decompositions*, Des. Codes Cryptogr. **47** (2008), no. 1-3, 289–303. MR MR2375474 (2008m:20004)
- [27] Gary J. Sherman, Thomas J. Tucker, and Mark E. Walker, *How Hamiltonian can a finite group be?*, Arch. Math. (Basel) **57** (1991), no. 1, 1–5. MR MR1111106 (92f:20026)
- [28] Bruce W. Westbury, *Invariant tensors and the cyclic sieving phenomenon*, 2010.
- [29] Doron Zeilberger, *Deconstructing the Zeilberger algorithm*, J. Difference Equ. Appl. **11** (2005), no. 9, 851–856. MR MR2159801 (2006i:05181)
- [30] Cui Zhang, Jin-Xin Zhou, and Yan-Quan Feng, *Automorphisms of cubic Cayley graphs of order  $2pq$* , Discrete Math. **309** (2009), no. 9, 2687–2695. MR MR2523776
- [31] Jin-Xin Zhou, *Tetravalent  $s$ -transitive graphs of order  $4p$* , Discrete Math. **309** (2009), no. 20, 6081–6086. MR MR2552643
- [32] Jin-Xin Zhou and Yan-Quan Feng, *Tetravalent one-regular graphs of order  $2pq$* , J. Algebraic Combin. **29** (2009), no. 4, 457–471. MR MR2506717
- [33] ———, *Tetravalent  $s$ -transitive graphs of order twice a prime power*, J. Aust. Math. Soc. **88** (2010), no. 2, 277–288.

# Computational Methods

05-04

- [1] David Abelson, Seok-Hee Hong, and D. E. Taylor, *Geometric automorphism groups of graphs*, Discrete Appl. Math. **155** (2007), no. 17, 2211–2226. MR MR2360651
- [2] David Abelson, Seok-Hee Hong, and Donald E. Taylor, *A group-theoretic method for drawing graphs symmetrically*, Graph Drawing, Lecture Notes in Comput. Sci., vol. 2528, Springer, Berlin, 2002, pp. 86–97. MR MR2063414
- [3] John M. Boyer and Wendy J. Myrvold, *On the cutting edge: Simplified  $O(n)$  planarity by edge addition*, J. Graph Algorithms Appl. **8** (2004), no. 3, 241–273 (electronic). MR MR2166815
- [4] Florent Hivert and Nicolas M. Thiéry, *MuPAD-Combinat, an open-source package for research in algebraic combinatorics*, Sém. Lothar. Combin. **51** (2004/05), Art. B51z, 70 pp. (electronic). MR MR2080390 (2005c:05001)
- [5] M. (ed.) Klin, G.A. (ed.) Jones, A. (ed.) Jurisic, M. (ed.) Muzychuk, and I. (ed.) Ponomarenko, *Algorithmic algebraic combinatorics and gröbner bases*, Springer, Berlin, 2009.
- [6] C. Koukouvinos and S. Stylianou, *On skew-Hadamard matrices*, Discrete Math. **308** (2008), no. 13, 2723–2731. MR MR2413970
- [7] Paulette Lieby, *Colouring planar graphs*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 315–330. MR MR2278934
- [8] Adolfo Piperno, *Search space contraction in canonical labeling of graphs (preliminary version)*, 2008.
- [9] Leonard H. Soicher, *Computing with graphs and groups*, Topics in algebraic graph theory (Lowell W. Beineke and Robin J. Wilson, eds.), Encyclopedia of Mathematics and its Applications, vol. 102, Cambridge University Press, Cambridge, 2004, pp. 250–266. MR MR2125091 (2005m:05002)
- [10] Kozo Sugiyama, Seok-Hee Hong, and Atsuhiko Maeda, *The puzzle layout problem*, Graph Drawing, Perugia, 2003 (Giuseppe Liotta, ed.), Springer, 2004, pp. 500–501.



- [11] Doron Zeilberger, *Deconstructing the Zeilberger algorithm*, J. Difference Equ. Appl. **11** (2005), no. 9, 851–856. MR MR2159801 (2006i:05181)

# Commutative Algebra

## Commutative Algebra: General

13Axx excluding 13A50, 13Bxx

- [1] David F. Anderson, Andrea Frazier, Aaron Lauve, and Philip S. Livingston, *The zero-divisor graph of a commutative ring: II*, Ideal Theoretic Methods in Commutative Algebra (Columbia, MO, 1999), Lecture Notes in Pure and Appl. Math., vol. 220, Dekker, New York, 2001, pp. 61–72. MR MR1836591 (2002e:13016)
- [2] David F. Anderson and Philip S. Livingston, *The zero-divisor graph of a commutative ring*, J. Algebra **217** (1999), no. 2, 434–447. MR MR1700509 (2000e:13007)
- [3] G. Chèze and S. Najib, *Indecomposability of polynomials via Jacobian matrix*, J. Algebra **324** (2010), no. 1, 1–11. MR 2646027
- [4] Robert S. Coulter, George Havas, and Marie Henderson, *On decomposition of sub-linearised polynomials*, J. Aust. Math. Soc. **76** (2004), no. 3, 317–328. MR MR2053506 (2005b:13013)
- [5] David A. Cox, John Little, and Donal O’Shea, *Using Algebraic Geometry*, second ed., Graduate Texts in Mathematics, vol. 185, Springer, New York, 2005. MR MR2122859 (2005i:13037)
- [6] Jan Draisma, Gregor Kemper, and David Wehlau, *Polarization of separating invariants*, Canad. J. Math. **60** (2008), no. 3, 556–571. MR MR2414957 (2009c:13011)
- [7] Douglas A. Leonard, *A weighted module view of integral closures of affine domains of type I*, Adv. Math. Commun. **3** (2009), no. 1, 1–11.
- [8] Miles Reid, *Graded rings and birational geometry*, 2000.
- [9] R. J. Shank, *Classical covariants and modular invariants*, Invariant Theory in all Characteristics, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 241–249. MR MR2066471 (2005d:13012)

# Invariant Theory

13A50

- [1] Thomas Bayer, *An algorithm for computing invariants of linear actions of algebraic groups up to a given degree*, J. Symbolic Comput. **35** (2003), no. 4, 441–449. MR MR1976577 (2004c:13045)
- [2] Dave Benson, *Dickson invariants, regularity and computation in group cohomology*, Illinois J. Math. **48** (2004), no. 1, 171–197. MR MR2048221 (2005c:20089)
- [3] Mireille Boutin and Gregor Kemper, *On reconstructing  $n$ -point configurations from the distribution of distances or areas*, Adv. in Appl. Math. **32** (2004), no. 4, 709–735. MR MR2053842 (2005c:68259)
- [4] ———, *On reconstructing configurations of points in  $P^2$  from a joint distribution of invariants*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), no. 6, 361–391. MR MR2134687 (2006a:13011)
- [5] Abraham Broer, *On Chevalley-Shephard-Todd’s theorem in positive characteristic*, Symmetry and Spaces (H. E. A. Campbell, Aloysius G. Helminck, Hanspeter Kraft, and David Wehlau, eds.), Progress in Mathematics, Birkhäuser Boston, 2010, pp. 21–34.
- [6] H. E. A. Campbell, B. Fodden, and David L. Wehlau, *Invariants of the diagonal  $C_p$ -action on  $V_3$* , J. Algebra **303** (2006), no. 2, 501–513. MR MR2255119 (2007f:13009)
- [7] H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, and D. L. Wehlau, *Depth of modular invariant rings*, Transform. Groups **5** (2000), no. 1, 21–34. MR MR1745709 (2001a:13004)
- [8] H. E. A. Campbell, R. J. Shank, and D. L. Wehlau, *Vector invariants for the two dimensional modular representation of a cyclic group of prime order*, Advances in Mathematics **225** (2010), no. 2, 1069–1094.
- [9] Chris Charnes, Martin Rötteler, and Thomas Beth, *On homogeneous bent functions*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 249–259. MR MR1913471 (2003e:94065)

- [10] ———, *Homogeneous bent functions, invariants, and designs*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 139–154. MR MR1919874 (2003h:05043)
- [11] Wolfram Decker and Theo de Jong, *Gröbner bases and invariant theory*, Gröbner bases and applications (Linz, 1998), London Math. Soc. Lecture Note Ser., vol. 251, Cambridge Univ. Press, Cambridge, 1998, pp. 61–89. MR MR1699814 (2000m:13007)
- [12] Harm Derksen, *Computation of invariants for reductive groups*, Adv. Math. **141** (1999), no. 2, 366–384. MR MR1671758 (2000a:13013)
- [13] Harm Derksen and Gregor Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, , Encyclopaedia of Mathematical Sciences, 130. MR MR1918599 (2003g:13004)
- [14] Emilie Dufresne, Jonathan Elmer, and Martin Kohls, *The Cohen-Macaulay property of separating invariants of finite groups*, Transform. Groups **14** (2009), no. 4, 771–785. MR MR2577197
- [15] Alexander Duncan, Michael LeBlanc, and David L. Wehlau, *A SAGBI basis for  $F[V_2 \oplus V_2 \oplus V_3]^{C_p}$* , Canad. Math. Bull. **52** (2009), no. 1, 72–83. MR MR2494313
- [16] Jonathan Elmer, *Depth and detection in modular invariant theory*, J. Algebra **322** (2009), no. 5, 1653–1666. MR MR2543628
- [17] Jonathan Elmer and Peter Fleischmann, *On the depth of modular invariant rings for the groups  $C_p \times C_p$* , Symmetry and Spaces, Progr. Math., vol. 278, Birkhäuser Boston Inc., Boston, MA, 2010, pp. 45–61. MR MR2562623
- [18] Tom Fisher, *The Hessian of a genus one curve*, 2006.
- [19] P. Fleischmann, M. Sezer, R. J. Shank, and C. F. Woodcock, *The Noether numbers for cyclic groups of prime order*, Adv. Math. **207** (2006), no. 1, 149–155. MR MR2264069 (2007e:13010)
- [20] Karin Gatermann and Frédéric Guyard, *Gröbner bases, invariant theory and equivariant dynamics*, J. Symbolic Comput. **28** (1999), no. 1-2, 275–302, Polynomial elimination—algorithms and applications. MR MR1709907 (2000f:13006)
- [21] Karin Gatermann and Pablo A. Parrilo, *Symmetry groups, semidefinite programs, and sums of squares*, J. Pure Appl. Algebra **192** (2004), no. 1-3, 95–128. MR MR2067190 (2005d:68155)

- [22] Ian Hughes and Gregor Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds*, *Comm. Algebra* **28** (2000), no. 4, 2059–2088. MR MR1747371 (2001b:13009)
- [23] ———, *Symmetric powers of modular representations for groups with a Sylow subgroup of prime order*, *J. Algebra* **241** (2001), no. 2, 759–788. MR MR1843324 (2002e:13012)
- [24] D. B. Karagueuzian and P. Symonds, *The module structure of a group action on a polynomial ring: Examples, generalizations, and applications*, *Invariant Theory in all Characteristics*, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 139–158. MR MR2066462 (2005g:13011)
- [25] Gregor Kemper, *Calculating invariants of modular reflection groups with Magma*, 1997.
- [26] ———, *Computational invariant theory*, *The Curves Seminar at Queen's. Vol. XII* (Kingston, ON, 1998), *Queen's Papers in Pure and Appl. Math.*, vol. 114, Queen's Univ., Kingston, ON, 1998, pp. 5–26. MR MR1690811 (2000c:13007)
- [27] ———, *The depth of invariant rings and cohomology*, *J. Algebra* **245** (2001), no. 2, 463–531, With an appendix by Kay Magaard. MR MR1863889 (2002h:13009)
- [28] ———, *Computing invariants of reductive groups in positive characteristic*, *Transform. Groups* **8** (2003), no. 2, 159–176. MR MR1976458 (2004b:13006)
- [29] ———, *The computation of invariant fields and a constructive version of a theorem by Rosenlicht*, *Transform. Groups* **12** (2007), no. 4, 657–670. MR MR2365439 (2008m:13011)
- [30] Gregor Kemper, Elmar Körding, Gunter Malle, B. Heinrich Matzat, Denis Vogel, and Gabor Wiese, *A database of invariant rings*, *Experiment. Math.* **10** (2001), no. 4, 537–542. MR MR1881754 (2002k:13011)
- [31] Gregor Kemper and Gunter Malle, *Invariant fields of finite irreducible reflection groups*, *Math. Ann.* **315** (1999), no. 4, 569–586. MR MR1731462 (2001c:13006)
- [32] Gregor Kemper and Allan Steel, *Some algorithms in invariant theory of finite groups*, *Computational Methods for Representations of Groups and Algebras* (Essen, 1997), *Progr. Math.*, vol. 173, Birkhäuser, Basel, 1999, pp. 267–285. MR MR1714617 (2000j:13009)

- [33] Simon King, *Fast computation of secondary invariants*, 2007.
- [34] ———, *Minimal generating sets of non-modular invariant rings of finite groups*, 2007.
- [35] Martin Kohls, *Invarianten zusammenhaengender gruppen und die Cohen-Macaulay eigenschaft*, Diplomarbeit, Technische Universitaet Muechen, 2005.
- [36] ———, *Üeber die tiefe von invariantenringen unendlicher gruppen*, PhD Thesis, Technische Universitaet Muechen, 2007.
- [37] Martin Kohls, *On the depth of invariant rings of infinite groups*, J. Algebra **322** (2009), no. 1, 210–218. MR MR2526384
- [38] P. H. Kropholler, S. Mohseni Rajaei, and J. Segal, *Invariant rings of orthogonal groups over  $\mathbf{F}_2$* , Glasg. Math. J. **47** (2005), no. 1, 7–54. MR MR2200953 (2006i:13009)
- [39] Martin Lorenz, *Multiplicative Invariant Theory*, Encyclopaedia of Mathematical Sciences, vol. 135, Springer-Verlag, Berlin, 2005, Invariant Theory and Algebraic Transformation Groups, VI. MR MR2131760 (2005m:13012)
- [40] A. Marschner and J. Müller, *On a certain algebra of higher modular forms*, Algebra Colloq. **16** (2009), 371–380.
- [41] Jürgen Müller and Christophe Ritzenthaler, *On the ring of invariants of ordinary quartic curves in characteristic 2*, J. Algebra **303** (2006), no. 2, 530–542. MR MR2255121
- [42] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane, *Self-dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR MR2209183
- [43] Mara D. Neusel and Müfit Sezer, *The invariants of modular indecomposable representations of  $Z_{p^2}$* , Math. Ann. **341** (2008), no. 3, 575–587. MR MR2399159 (2009b:13007)
- [44] W. Plesken and D. Robertz, *Constructing invariants for finite groups*, Experiment. Math. **14** (2005), no. 2, 175–188. MR MR2169521
- [45] Marc Stetson Renault, *Computing Generators for Rings of Multiplicative Invariants*, PhD Thesis, Temple University, 2002.
- [46] Müfit Sezer and R. James Shank, *On the coinvariants of modular representations of cyclic groups of prime order*, J. Pure Appl. Algebra **205** (2006), no. 1, 210–225. MR MR2193198

- [47] R. J. Shank, *Classical covariants and modular invariants*, Invariant Theory in all Characteristics, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 241–249. MR MR2066471 (2005d:13012)
- [48] R. James Shank and David L. Wehlau, *On the depth of the invariants of the symmetric power representations of  $SL_2(\mathbf{F}_p)$* , J. Algebra **218** (1999), no. 2, 642–653. MR MR1705766 (2000f:13010)
- [49] ———, *Computing modular invariants of  $p$ -groups*, J. Symbolic Comput. **34** (2002), no. 5, 307–327. MR MR1937464 (2003j:13006)
- [50] ———, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002), no. 4, 438–450. MR MR1897423 (2003a:13005)
- [51] ———, *Decomposing symmetric powers of certain modular representations of cyclic groups*, Progress in Mathematics **278** (2010), 169–196.
- [52] Nicolas M. Thiéry, *Algebraic invariants of graphs; A study based on computer exploration*, SIGSAM Bulletin **34** (2000), no. 3, 9–20.

# Modules and Ideals

13Cxx

- [1] Jon F. Carlson, *Cohomology, computations, and commutative algebra*, Notices Amer. Math. Soc. **52** (2005), no. 4, 426–434. MR MR2127572 (2006f:20061)
- [2] Gregor Kemper, *The depth of invariant rings and cohomology*, J. Algebra **245** (2001), no. 2, 463–531, With an appendix by Kay Magaard. MR MR1863889 (2002h:13009)
- [3] R. James Shank and David L. Wehlau, *On the depth of the invariants of the symmetric power representations of  $SL_2(\mathbf{F}_p)$* , J. Algebra **218** (1999), no. 2, 642–653. MR MR1705766 (2000f:13010)
- [4] Arno van den Essen, Andrzej Nowicki, and Andrzej Tyc, *Generalizations of a lemma of Freudenburg*, J. Pure Appl. Algebra **177** (2003), no. 1, 43–47. MR MR1948836 (2003m:13017)



# Homological Methods

13Dxx

- [1] Selma Altınok, Gavin Brown, and Miles Reid, *Fano 3-folds, K3 surfaces and graded rings*, Topology and Geometry: Commemorating SISTAG, Contemp. Math., vol. 314, Amer. Math. Soc., Providence, RI, 2002, pp. 25–53. MR MR1941620 (2004c:14077)
- [2] Gavin Brown, *Graded rings and special K3 surfaces*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 137–159. MR MR2278926
- [3] Laurent Busé and Jean-Pierre Jouanolou, *On the closed image of a rational map and the implicitization problem*, J. Algebra **265** (2003), no. 1, 312–357. MR MR1984914 (2004e:14024)
- [4] Jeffrey B. Farr and Shuhong Gao, *Computing Gröbner bases for vanishing ideals of finite sets of points*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes, Lecture Notes in Comput. Sci., vol. 3857, Springer, Berlin, 2006, pp. 118–127. MR MR2243500 (2007c:13039)
- [5] Ian Hughes and Gregor Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds*, Comm. Algebra **28** (2000), no. 4, 2059–2088. MR MR1747371 (2001b:13009)
- [6] ———, *Symmetric powers of modular representations for groups with a Sylow subgroup of prime order*, J. Algebra **241** (2001), no. 2, 759–788. MR MR1843324 (2002e:13012)
- [7] Mikael Johansson, *Computation of Poincaré-Betti series for monomial rings*, Rend. Istit. Mat. Univ. Trieste **37** (2005), no. 1-2, 85–94 (2006). MR MR2227050 (2007b:13020)
- [8] Gregor Kemper, *Computational invariant theory*, The Curves Seminar at Queen’s. Vol. XII (Kingston, ON, 1998), Queen’s Papers in Pure and Appl. Math., vol. 114, Queen’s Univ., Kingston, ON, 1998, pp. 5–26. MR MR1690811 (2000c:13007)
- [9] Gregor Kemper and Allan Steel, *Some algorithms in invariant theory of finite groups*, Computational Methods for Representations of Groups and Algebras (Essen, 1997), Progr. Math., vol. 173, Birkhäuser, Basel, 1999, pp. 267–285. MR MR1714617 (2000j:13009)

- [10] Peter Symonds, *Cyclic group actions on polynomial rings*, Bull. Lond. Math. Soc. **39** (2007), no. 2, 181–188. MR MR2323446

# Differential Algebra

12H05, 13Nxx

- [1] Alin Bostan, Frédéric Chyzak, and Nicolas Le Roux, *Products of ordinary differential operators by evaluation and interpolation*, ISSAC '08: International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM, 2008, pp. 23–30.
- [2] Alin Bostan, Frédéric Chyzak, Bruno Salvy, Grégoire Lecerf, and Éric Schost, *Differential equations for algebraic functions*, ISSAC 2007, ACM, New York, 2007, pp. 25–32. MR MR2396180
- [3] Alin Bostan, Thomas Cluzeau, and Bruno Salvy, *Fast algorithms for polynomial solutions of linear differential equations*, ISSAC'05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 45–52 (electronic). MR MR2280528
- [4] Olivier Cormier, *On Liouvillian solutions of linear differential equations of order 4 and 5*, ISSAC '01: Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2001, pp. 93–100 (electronic). MR MR2049736
- [5] Olivier Cormier, Michael F. Singer, and Felix Ulmer, *Computing the Galois group of a polynomial using linear differential equations*, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews) (New York), ACM, 2000, pp. 78–85 (electronic). MR MR1805111 (2002f:12008)
- [6] Boris Feigin and Boris Shoikhet, *On  $[A, A]/[A, [A, A]]$  and on a  $W_n$ -action on the consecutive commutators of free associative algebra*, Math. Res. Lett. **14** (2007), no. 5, 781–795. MR MR2350124 (2009b:16055)
- [7] Julia Hartmann, *Invariants and differential Galois groups in degree four*, Differential Galois Theory, Banach Center Publ., vol. 58, Polish Acad. Sci., Warsaw, 2002, pp. 79–87. MR MR1972447 (2004c:12011)
- [8] Sabrina A. Hessinger, *Computing the Galois group of a linear differential equation of order four*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 489–536. MR MR1831942 (2002c:12009)

- [9] V.A. Krasikov and T.M. Sadykov, *Linear differential operators for generic algebraic curves*, 2010.
- [10] Ariane Péladan-Germa, *Testing equality in differential ring extensions defined by PDE's and limit conditions*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 4, 257–288. MR MR1953194 (2003k:12010)
- [11] Kira Samol and Duco van Straten, *Frobenius polynomials for Calabi-Yau equations*, Commun. Number Theory Phys. **2** (2008), no. 3, 537–561. MR MR2482942
- [12] Michael F. Singer, *Testing reducibility of linear differential operators: A group-theoretic perspective*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 2, 77–104. MR MR1462491 (98e:12007)
- [13] Michael F. Singer and Felix Ulmer, *Galois groups of second and third order linear differential equations*, J. Symbolic Comput. **16** (1993), no. 1, 9–36. MR MR1237348 (94i:34015)
- [14] ———, *Liouvillian and algebraic solutions of second and third order linear differential equations*, J. Symbolic Comput. **16** (1993), no. 1, 37–73. MR MR1237349 (94i:34016)
- [15] ———, *On a third order differential equation whose differential Galois group is the simple group of 168 elements*, Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., vol. 673, Springer, Berlin, 1993, pp. 316–324. MR MR1251988 (95e:34010)
- [16] ———, *Necessary conditions for Liouvillian solutions of (third order) linear differential equations*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), no. 1, 1–22. MR MR1341890 (96j:34005)
- [17] Felix Ulmer, *On algebraic solutions of linear differential equations with primitive unimodular Galois group*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (New Orleans, LA, 1991), Lecture Notes in Comput. Sci., vol. 539, Springer, Berlin, 1991, pp. 446–455. MR MR1229340 (94e:68094)
- [18] ———, *On Liouvillian solutions of linear differential equations*, Appl. Algebra Engrg. Comm. Comput. **2** (1992), no. 3, 171–193. MR MR1325527 (96e:12007)
- [19] ———, *Liouvillian solutions of third order differential equations*, J. Symbolic Comput. **36** (2003), no. 6, 855–889. MR MR2021282 (2004k:34007)

# Computational Methods

13-04

- [1] I. Abdeljaouad-Tej, S. Orange, G. Renault, and A. Valibouze, *Computation of the decomposition group of a triangular ideal*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 3-4, 279–294. MR MR2104299 (2005h:13036)
- [2] Fatima Abu Salem, Shuhong Gao, and Alan G. B. Lauder, *Factoring polynomials via polytopes*, ISSAC 2004, ACM, New York, 2004, pp. 4–11. MR MR2126918 (2006a:13040)
- [3] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita, *Comparison between XL and Gröbner basis algorithms*, Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Comput. Sci., vol. 3329, Springer, Berlin, 2004, pp. 338–353. MR MR2150425 (2006k:13056)
- [4] Philippe Aubry and Marc Moreno Maza, *Triangular sets for solving polynomial systems: A comparative implementation of four methods*, J. Symbolic Comput. **28** (1999), no. 1-2, 125–154, Polynomial elimination—algorithms and applications. MR MR1709420 (2000g:13017)
- [5] Mohamed Ayad and Peter Fleischmann, *On the decomposition of rational functions*, J. Symbolic Comput. **43** (2008), no. 4, 259–274. MR MR2402031 (2009a:13047)
- [6] Bernd Bank, Marc Giusti, Joos Heintz, Mohab Safey El Din, and Eric Schost, *On the geometry of polar varieties*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 1, 33–83. MR 2585564
- [7] Aurélie Bauer and Antoine Joux, *Toward a rigorous variation of Coppersmith’s algorithm on three variables*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 361–378. MR MR2449220
- [8] Karim. Belabas, Mark van Hoeij, J. Klüners, and Allan Steel, *Factoring polynomials over global fields*, Journal de Théorie des Nombres de Bordeaux (2009), no. 21, 15–39.
- [9] Thomas Beth, Jörn Müller-Quade, and Rainer Steinwandt, *Computing restrictions of ideals in finitely generated  $k$ -algebras by means of Buchberger’s algorithm*, J. Symbolic Comput. **41** (2006), no. 3-4, 372–380. MR MR2202557 (2006j:13027)

- [10] Alin Bostan, Bruno Salvy, and Éric Schost, *Fast algorithms for zero-dimensional polynomial systems using duality*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 4, 239–272. MR MR2020362 (2005b:13050)
- [11] Richard Brent and Paul Zimmermann, *A multi-level blocking distinct degree factorization algorithm*, Finite Fields and Applications, Contemporary Mathematics, vol. 461, 2008.
- [12] Michael Brickenstein and Alexander Dreyer, *PolyBoRi: A framework for Gröbner-basis computations with Boolean polynomials*, J. Symbolic Comp. **44** (2009), no. 9, 1326–1345.
- [13] Michael Brickenstein, Alexander Dreyer, Gert-Martin Greuel, Markus Wedler, and Oliver Wienand, *New developments in the theory of Gröbner bases and applications to formal verification*, J. Pure Appl. Algebra **213** (2009), no. 8, 1612–1635. MR MR2517997
- [14] Stanislav Bulygin and Ruud Pellikaan, *Bounded distance decoding of linear error-correcting codes with Gröbner bases*, J. Symb. Comput. **44** (2009), no. 12, 1626–1643.
- [15] Daniel Cabarcas, *An Implementation of Faugère’s  $F_4$  Algorithm for Computing Gröbner Bases*, Master of Science Thesis, University of Cincinnati, 2010.
- [16] G. Chèze and S. Najib, *Indecomposability of polynomials via Jacobian matrix*, J. Algebra **324** (2010), no. 1, 1–11. MR 2646027
- [17] Mihai Cipu, *Gröbner bases and Diophantine analysis*, J. Symbolic Comput. **43** (2008), no. 10, 681–687. MR MR2426566
- [18] Jennifer de Kleine, Michael Monagan, and Allan Wittkopf, *Algorithms for the non-monic case of the sparse modular GCD algorithm*, Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation: ISSAC’05, ACM, New York, 2005, pp. 124–131 (electronic). MR MR2280538
- [19] Wolfram Decker and Theo de Jong, *Gröbner bases and invariant theory*, Gröbner bases and applications (Linz, 1998), London Math. Soc. Lecture Note Ser., vol. 251, Cambridge Univ. Press, Cambridge, 1998, pp. 61–89. MR MR1699814 (2000m:13007)
- [20] Harm Derksen, *Computation of invariants for reductive groups*, Adv. Math. **141** (1999), no. 2, 366–384. MR MR1671758 (2000a:13013)

- [21] Harm Derksen and Gregor Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, , Encyclopaedia of Mathematical Sciences, 130. MR MR1918599 (2003g:13004)
- [22] Clémence Durvye and Grégoire Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Expo. Math. **26** (2008), no. 2, 101–139. MR MR2413831
- [23] Tobias Eibach, Enrico Pilz, and Gunnar Völkel, *Attacking Bivium using SAT solvers*, Theory and Applications of Satisfiability Testing, SAT 2008, Lecture Notes in Computer Science, vol. 4996, Springer, Berlin, 2008, pp. 63–76.
- [24] Tobias Eibach, Gunnar Völkel, and Enrico Pilz, *Optimising Gröbner bases on Bivium*, Math. Comput. Sci. **3** (2010), no. 2, 159–172.
- [25] Nicholas Eriksson, *Toric ideals of homogeneous phylogenetic models*, ISSAC 2004, ACM, New York, 2004, pp. 149–154. MR MR2126937 (2005j:92017)
- [26] Jeffrey B. Farr and Shuhong Gao, *Computing Gröbner bases for vanishing ideals of finite sets of points*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes, Lecture Notes in Comput. Sci., vol. 3857, Springer, Berlin, 2006, pp. 118–127. MR MR2243500 (2007c:13039)
- [27] ———, *Gröbner bases and generalized Padé approximation*, Math. Comp. **75** (2006), no. 253, 461–473 (electronic). MR MR2176409
- [28] Jean-Charles Faugère, Guillaume Moroz, Fabrice Rouillier, and Mohab Safey El Din, *Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities*, ISSAC '08: International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM, 2008, pp. 79–86.
- [29] Akpodigha Filatei, *Implementation of fast polynomial arithmetic in Aldor*, Master of Science thesis, University of Western Ontario, 2006.
- [30] Shuhong Gao, Daqing Wan, and Mingsheng Wang, *Primary decomposition of zero-dimensional ideals over finite fields*, Math. Comp. **78** (2009), no. 265, 509–521. MR MR2448718
- [31] Karin Gatermann, *Computer algebra methods for equivariant dynamical systems*, Lecture Notes in Mathematics, vol. 1728, Springer-Verlag, Berlin, 2000. MR MR1755001 (2001k:37040)

- [32] Karin Gatermann and Frédéric Guyard, *Gröbner bases, invariant theory and equivariant dynamics*, J. Symbolic Comput. **28** (1999), no. 1-2, 275–302, Polynomial elimination—algorithms and applications. MR MR1709907 (2000f:13006)
- [33] V. P. Gerdt and Yu. A. Blinkov, *On selection of nonmultiplicative prolongations in computation of Janet bases*, Programming and Computer Software **33** (2007), no. 3, 147–153.
- [34] V. P. Gerdt and Yu. A. Blinkov, *Strategies for selecting non-multiplicative prolongations in computing Janet bases*, Programmirovaniye (2007), no. 3, 34–43. MR MR2347312
- [35] Vladimir P. Gerdt, *Involutive algorithms for computing Gröbner bases*, Computational Commutative and Non-commutative Algebraic Geometry, NATO Sci. Ser. III Comput. Syst. Sci., vol. 196, IOS, Amsterdam, 2005, pp. 199–225. MR MR2179201
- [36] Vladimir P. Gerdt and Yuri A. Blinkov, *On computing Janet bases for degree compatible orderings*, Proceedings of the 10th Rhine Workshop on Computer Algebra (Basel), 2006, University of Basel, Basel, 2006, pp. 107–117.
- [37] Massimo Giulietti, *Involuppi di  $k$ -archi in piani proiettivi sopra campi finiti e basi di Gröbner*, Rendiconti del Circolo Matematico di Palermo **48** (1999), no. 1, 191–200.
- [38] Marc Giusti, Grégoire Lecerf, and Bruno Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity **17** (2001), no. 1, 154–211. MR MR1817612 (2002b:68123)
- [39] Marc Giusti and Éric Schost, *Solving some overdetermined polynomial systems*, ISSAC '99: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 1–8 (electronic). MR MR1802060 (2002b:65084)
- [40] Hoans-Christian Graf von Bothmer, Oliver Labs, Josef Schicho, and Christiaan van de Woestijne, *The Casas-Alvero conjecture for infinitely many degrees*, J. Algebra **316** (2007), no. 1, 224–230. MR MR2354861
- [41] Gert-Martin Greuel, Santiago Laplagne, and Frank Seelisch, *Normalization of rings*, J. Symbolic Comput. **45** (2010), no. 9, 887–901.



- [42] Renault Guénaél and Yokoyama Kazuhiro, *Multi-modular algorithm for computing the splitting field of a polynomial*, ISSAC '08: International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM, 2008, pp. 247–254.
- [43] David Harvey, *A cache-friendly truncated FFT*, Theor. Comput. Sci. **410** (2009), no. 27-29, 2649–2658.
- [44] David Harvey, *Faster polynomial multiplication via multipoint Kronecker substitution*, J. Symbolic Comp. **44** (2009), no. 10, 1502–1510.
- [45] Mikael Johansson, *Computation of Poincaré-Betti series for monomial rings*, Rend. Istit. Mat. Univ. Trieste **37** (2005), no. 1-2, 85–94 (2006). MR MR2227050 (2007b:13020)
- [46] Gregor Kemper, *Computational invariant theory*, The Curves Seminar at Queen's. Vol. XII (Kingston, ON, 1998), Queen's Papers in Pure and Appl. Math., vol. 114, Queen's Univ., Kingston, ON, 1998, pp. 5–26. MR MR1690811 (2000c:13007)
- [47] ———, *An algorithm to calculate optimal homogeneous systems of parameters*, J. Symbolic Comput. **27** (1999), no. 2, 171–184. MR MR1672128 (2000a:13046)
- [48] ———, *The calculation of radical ideals in positive characteristic*, J. Symbolic Comput. **34** (2002), no. 3, 229–238. MR MR1935080 (2003j:13039)
- [49] ———, *Computing invariants of reductive groups in positive characteristic*, Transform. Groups **8** (2003), no. 2, 159–176. MR MR1976458 (2004b:13006)
- [50] Simon King, *Fast computation of secondary invariants*, 2007.
- [51] ———, *Minimal generating sets of non-modular invariant rings of finite groups*, 2007.
- [52] Alexey Koloydenko, *Symmetric measures via moments*, Bernoulli **14** (2008), no. 2, 362–390.
- [53] Teresa Krick, *Straight-line programs in polynomial equation solving*, Foundations of Computational Mathematics: Minneapolis, 2002, London Math. Soc. Lecture Note Ser., vol. 312, Cambridge Univ. Press, Cambridge, 2004, pp. 96–136. MR MR2189629
- [54] G. Lecerf, *Quadratic Newton iteration for systems with multiplicity*, Found. Comput. Math. **2** (2002), no. 3, 247–293. MR MR1907381 (2003f:65090)

- [55] Grégoire Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, J. Complexity **19** (2003), no. 4, 564–596. MR MR1991984 (2004j:68200)
- [56] ———, *Fast separable factorization and applications*, Appl. Algebra Engrg. Comm. Comput. **19** (2008), no. 2, 135–160. MR MR2389971 (2009b:13069)
- [57] ———, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 2, 151–176. MR 2600710
- [58] Xin Li, Marc Moreno Maza, Raqeeb Rasheed, and Eric Schost, *High-performance symbolic computation in a hybrid compiled-interpreted programming environment*, International Conference on Computational Sciences and Its Applications. ICCSA. June 30- July 3, 2008, 2008, pp. 331–341.
- [59] Xin Li, Marc Moreno Maza, and Éric Schost, *Fast arithmetic for triangular sets: from theory to practice*, ISSAC 2007, ACM, New York, 2007, pp. 269–276. MR MR2402271
- [60] Xin Li, Marc Moreno Maza, and Éric Schost, *Fast arithmetic for triangular sets: from theory to practice*, J. Symbolic Comput. **44** (2009), no. 7, 891–907. MR MR2522589
- [61] A. Marschner and J. Müller, *On a certain algebra of higher modular forms*, Algebra Colloq. **16** (2009), 371–380.
- [62] Mbakop Guy Merlin, *Eziente losung reeller polynomialer gleichungssysteme*, PhD Thesis, Humboldt-Universität, Berlin, 1999.
- [63] V. A. Mityunin and E. V. Pankratiev, *Parallel algorithms for Gröbner-basis construction*, J. Math. Sci. (N. Y.) **142** (2007), no. 4, 2248–2266.
- [64] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions*.
- [65] Teo Mora, *The FGLM problem and Möller’s algorithm on zero-dimensional ideals*, Sala, Massimiliano (ed.) and Mora, Teo (ed.) and Perret, Ludovic (ed.) and Sakata, Shojiro (ed.) and Traverso, Carlo (ed.), Gröbner Bases, Coding, and Cryptography, Springer, Berlin, 2009.

- [66] Marc Moreno Maza, Greg Reid, Robin Scott, and Wenyuan Wu, *On approximate triangular decompositions in dimension zero*, J. Symbolic Comput. **42** (2007), no. 7, 693–716. MR MR2348057
- [67] Bernard Mourrain, *Generalized normal forms and polynomial system solving*, IS-SAC'05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 253–260 (electronic). MR MR2280555
- [68] Bernard Mourrain and Philippe Trébuchet, *Stable normal forms for polynomial system solving*, Theoret. Comput. Sci. **409** (2008), no. 2, 229–240. MR MR2474338 (2009m:13036)
- [69] Jörn Müller-Quade and Rainer Steinwandt, *Basic algorithms for rational function fields*, J. Symbolic Comput. **27** (1999), no. 2, 143–170. MR MR1672124 (2000a:13043)
- [70] ———, *Gröbner bases applied to finitely generated field extensions*, J. Symbolic Comput. **30** (2000), no. 4, 469–490. MR MR1784753 (2001i:13040)
- [71] G. H. Norton and A. Salagean, *Cyclic codes and minimal strong Gröbner bases over a principal ideal ring*, Finite Fields Appl. **9** (2003), no. 2, 237–249. MR MR1968033 (2004d:13039)
- [72] Graham H. Norton and Ana Sălăgean, *Strong Gröbner bases for polynomials over a principal ideal ring*, Bull. Austral. Math. Soc. **64** (2001), no. 3, 505–528. MR MR1878902 (2003a:13036)
- [73] Daniel Robertz, *Noether normalization guided by monomial cone decompositions*, J. Symbolic Comput. **44** (2009), no. 10, 1359–1373. MR MR2543424
- [74] Fabrice Rouillier, Mohab Safey El Din, and Éric Schost, *Solving the Birkhoff interpolation problem via the critical point method: An experimental study*, ADG '00: Revised Papers from the Third International Workshop on Automated Deduction in Geometry (Zurich, 2000) (Jürgen Richter-Gebert and Dongming Wang, eds.), Lecture Notes in Computer Science, vol. 2061, Springer-Verlag, Berlin, 2001, Lecture Notes in Artificial Intelligence, pp. viii+325. MR MR1908025 (2003a:68007)
- [75] Luciano Sbaiz, Patrick Vandewalle, and Martin Vetterli, *Groebner basis methods for multichannel sampling with unknown offsets*, Appl. Comput. Harmon. Anal. **25** (2008), no. 3, 277 – 294.

- [76] Roberto La Scala and Viktor Levandovskyy, *Letterplace ideals and non-commutative Gröbner bases*, J. Symbolic Comp. **44** (2009), no. 10, 1374–1393.
- [77] Éric Schost, *Degree bounds and lifting techniques for triangular sets*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2002, pp. 238–245 (electronic). MR MR2035255 (2005a:13054)
- [78] ———, *Complexity results for triangular sets*, J. Symbolic Comput. **36** (2003), no. 3–4, 555–594, International Symposium on Symbolic and Algebraic Computation (ISSAC’2002) (Lille). MR MR2004042 (2004m:68295)
- [79] ———, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), no. 5, 349–393. MR MR1959170 (2003k:13035)
- [80] R. James Shank and David L. Wehlau, *Computing modular invariants of  $p$ -groups*, J. Symbolic Comput. **34** (2002), no. 5, 307–327. MR MR1937464 (2003j:13006)
- [81] Jessica Sidman and Seth Sullivant, *Prolongations and computational algebra*, Canad. J. Math. **61** (2009), no. 4, 930–949. MR MR2541390
- [82] Allan Steel, *Conquering inseparability: Primary decomposition and multivariate factorization over algebraic function fields of positive characteristic*, J. Symbolic Comput. **40** (2005), no. 3, 1053–1075. MR MR2167699
- [83] Till Stegers, *Faugère’s F5 algorithm revisited*, Masters thesis, Technische Universität Darmstadt, 2005.
- [84] Rainer Steinwandt, *Decomposing systems of polynomial equations*, Computer Algebra in Scientific Computing—CASC’99 (Munich), Springer, Berlin, 1999, pp. 387–407. MR MR1729638 (2000j:12012)
- [85] ———, *Implicitizing without tag variables*, Proceedings of the 8th Rhine Workshop on Computer Algebra, 2002, pp. 217–224.
- [86] Rainer Steinwandt and Jörn Müller-Quade, *Freeness, linear disjointness, and implicitization—a classical approach*, Beiträge Algebra Geom. **41** (2000), no. 1, 57–66. MR MR1745579 (2001a:12011)
- [87] Mark van Hoeij, *Factoring polynomials and the knapsack problem*, J. Number Theory **95** (2002), no. 2, 167–189. MR MR1924096 (2003f:13029)

- [88] Pawel Wocjan, *Brill-Noether algorithm construction of geometric Goppa codes and absolute factorization of polynomials*, Ph.D. thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 1999, p. 108.

# Field Theory

## Field Theory: General

12Exx

- [1] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang, *A trace conjecture and flag-transitive affine planes*, J. Combin. Theory Ser. A **95** (2001), no. 1, 158–168. MR MR1840482 (2002c:11166)
- [2] B. V. Petrenko, *On the product of two primitive elements of maximal subfields of a finite field*, J. Pure Appl. Algebra **178** (2003), no. 3, 297–306. MR MR1953735 (2004b:11165)
- [3] ———, *On the sum of two primitive elements of maximal subfields of a finite field*, Finite Fields Appl. **9** (2003), no. 1, 102–116. MR MR1954786 (2003m:12004)
- [4] Ruth Schwingel, *The tensor product of polynomials*, Experiment. Math. **8** (1999), no. 4, 395–397. MR MR1737234 (2000j:12004)
- [5] Kirby C. Smith and Leon van Wyk, *A concrete matrix field description of some Galois fields*, Linear Algebra Appl. **403** (2005), 159–164. MR MR2140278 (2006b:12002)

# Extensions and Galois Theory

12Fxx

- [1] Alejandro Adem, Wenfeng Gao, Dikran B. Karagueuzian, and Ján Mináč, *Field theory and the cohomology of some Galois groups*, J. Algebra **235** (2001), no. 2, 608–635. MR MR1805473 (2001m:12011)
- [2] Maximilian Albert and Annette Maier, *Additive polynomials for finite groups of Lie type*, 2009.
- [3] Bill Allombert, *An efficient algorithm for the computation of Galois automorphisms*, Math. Comp. **73** (2004), no. 245, 359–375 (electronic). MR MR2034127 (2004k:11193)
- [4] Johan Bosman, *A polynomial with Galois group  $SL_2(F_{16})$* , LMS J. Comput. Math. **10** (2007), 1461–1570 (electronic). MR MR2365691
- [5] Nigel Boston, *Reducing the Fontaine-Mazur conjecture to group theory*, Progress in Galois theory, Dev. Math., vol. 12, Springer, New York, 2005, pp. 39–50. MR MR2148459
- [6] Nigel Boston and Charles Leedham-Green, *Explicit computation of Galois  $p$ -groups unramified at  $p$* , J. Algebra **256** (2002), no. 2, 402–413. MR MR1939112 (2003k:12004)
- [7] Nigel Boston and Harris Nover, *Computing pro- $p$ -Galois groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 1–10. MR MR2282911
- [8] Nigel Boston and David Perry, *Maximal 2-extensions with restricted ramification*, J. Algebra **232** (2000), no. 2, 664–672. MR MR1792749 (2001k:12005)
- [9] Antoine Colin, *Relative resolvents and partition tables in Galois group computations*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI) (New York), ACM, 1997, pp. 78–84 (electronic). MR MR1809973 (2001j:12001)
- [10] Lassina Dembélé, *A non-solvable Galois extension of  $Q$  ramified at 2 only*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 3-4, 111–116. MR MR2538094
- [11] Michael Dettweiler, *Galois realizations of classical groups and the middle convolution*, 2006.

- [12] Pilar Fernandez-Ferreiros and M. Angeles Gomez-Molleda, *Deciding the nilpotency of the Galois group by computing elements in the centre*, Math. Comp. **73** (2004), no. 248, 2043–2060 (electronic). MR MR2059750 (2005c:12005)
- [13] Louis Granboulan, *Construction d’une extension régulière de  $\mathbf{Q}(T)$  de groupe de Galois  $M_{24}$* , Experiment. Math. **5** (1996), no. 1, 3–14. MR MR1412950 (98c:12006)
- [14] Farshid Hajir, *On the Galois group of generalized Laguerre polynomials*, J. Théor. Nombres Bordeaux **17** (2005), no. 2, 517–525. MR MR2211305 (2006k:11218)
- [15] ———, *Tame pro- $p$  Galois groups: A survey of recent work*, Arithmetic, Geometry and Coding Theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 111–124. MR MR2182839
- [16] Emmanuel Hallouin, *Study and computation of a Hurwitz space and totally real  $\mathrm{PSL}_2(F_8)$ -extensions of  $Q$* , J. Algebra **292** (2005), no. 1, 259–281. MR MR2166804 (2006h:14041)
- [17] G. Hanrot and F. Morain, *Solvability by radicals from an algorithmic point of view*, Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2001, pp. 175–182 (electronic). MR MR2049746 (2005a:11200)
- [18] Florent Jouve, Emmanuel Kowalski, and David Zywina, *An explicit integral polynomial whose splitting field has galois group  $W(E_8)$* , J. Théor. Nombres Bordeaux **20** (2008), no. 3, 761–782. MR MR2523316
- [19] Gregor Kemper and Gunter Malle, *Invariant fields of finite irreducible reflection groups*, Math. Ann. **315** (1999), no. 4, 569–586. MR MR1731462 (2001c:13006)
- [20] Masanari Kida, Guénaél Renault, and Kazuhiro Yokoyama, *Quintic polynomials of Hashimoto-Tsunogai, Brumer and Kummer*, Int. J. Number Theory **5** (2009), no. 4, 555–571. MR MR2532276
- [21] Jürgen Klüners and Gunter Malle, *Explicit Galois realization of transitive groups of degree up to 15*, J. Symbolic Comput. **30** (2000), no. 6, 675–716, Algorithmic methods in Galois theory. MR MR1800033 (2001i:12005)
- [22] Aristides Kontogeorgis, *The group of automorphisms of cyclic extensions of rational function fields*, J. Algebra **216** (1999), no. 2, 665–706. MR MR1692965 (2000f:12005)



- [23] Jörn Müller-Quade and Rainer Steinwandt, *Recognizing simple subextensions of purely transcendental field extensions*, Appl. Algebra Engrg. Comm. Comput. **11** (2000), no. 1, 35–41. MR MR1817697 (2002g:12004)
- [24] Renault Guénaél Renault, *Computation of the splitting field of a dihedral polynomial*, ISSAC '06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 2006, pp. 290–297.
- [25] Núria Vila Sara Arias-de Reyna, *Tame Galois realizations of  $GSp_4(F_l)$  over  $Q$* , 2009.
- [26] Romyar T. Sharifi, *On Galois groups of unramified pro- $p$  extensions*, Math. Ann. **342** (2008), no. 2, 297–308. MR MR2425144
- [27] Blair K. Spearman, Kenneth S. Williams, and Qiduan Yang, *The 2-power degree subfields of the splitting fields of polynomials with Frobenius Galois groups*, Comm. Algebra **31** (2003), no. 10, 4745–4763. MR MR1998026 (2004f:12001)
- [28] Rainer Steinwandt and Jörn Müller-Quade, *Freeness, linear disjointness, and implicitization—a classical approach*, Beiträge Algebra Geom. **41** (2000), no. 1, 57–66. MR MR1745579 (2001a:12011)

# Semifields and Near-fields

12Kxx

- [1] Simeon Ball, Gary Ebert, and Michel Lavrauw, *A geometric construction of finite semifields*, J. Algebra **311** (2007), no. 1, 117–129. MR MR2309880
- [2] Robert S. Coulter and Marie Henderson, *Commutative presemifields and semifields*, Adv. Math. **217** (2008), no. 1, 282–304. MR MR2365198
- [3] Robert S. Coulter, Marie Henderson, and Pamela Kosick, *Planar polynomials for commutative semifields with specified nuclei*, Des. Codes Cryptogr. **44** (2007), no. 1-3, 275–286. MR MR2336411
- [4] G. L. Ebert, O. Polverino, G. Marino, and R. Trombetti, *Semifields in class  $F_4^{(a)}$* , Electron. J. Combin. **16** (2009), no. 1, 20. MR MR2505095
- [5] Gary L. Ebert, Giuseppe Marino, Olga Polverino, and Rocco Trombetti, *On the multiplication of some semifields of order  $q^6$* , Finite Fields Appl. **15** (2009), no. 2, 160–173. MR MR2494332
- [6] Jill Hanson and Michael J. Kallaher, *Finite Bol quasifields are nearfields*, Utilitas Math. **37** (1990), 45–64. MR MR1068509 (92b:51024)
- [7] K. J. Horadam and D. G. Farmer, *Bundles, presemifields and nonlinear functions*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 79–94. MR MR2438442
- [8] Norman L. Johnson, Giuseppe Marino, Olga Polverino, and Rocco Trombetti, *On a generalization of cyclic semifields*, J. Algebraic Combin. **29** (2009), no. 1, 1–34. MR MR2470113 (2010e:12010)
- [9] Giuseppe Marino and Rocco Trombetti, *A new semifield of order  $2^{10}$* , Discrete Math. **310** (2010), no. 22, 3108–3113.
- [10] I. F. Rúa, Elías F. Combarro, and J. Ranilla, *Classification of semifields of order 64*, J. Algebra **322** (2009), no. 11, 4011–4029. MR MR2556135

# Computational Methods

12-04

- [1] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson, *Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over  $\text{GF}(2)$  via SAT-solvers*, 2007.
- [2] Cristina Bertone, Guillaume Chéze, and André Galligo, *Modular Las Vegas algorithms for polynomial absolute factorization*, J. Symbolic Comput. **45** (2010), no. 12, 1280–1295.
- [3] Thomas Beth, Jörn Müller-Quade, and Rainer Steinwandt, *Computing restrictions of ideals in finitely generated  $k$ -algebras by means of Buchberger’s algorithm*, J. Symbolic Comput. **41** (2006), no. 3-4, 372–380. MR MR2202557 (2006j:13027)
- [4] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt, *Complexity issues in bivariate polynomial factorization*, ISSAC ’04: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 2004, pp. 42–49.
- [5] Guillaume Chéze and Grégoire Lecerf, *Lifting and recombination techniques for absolute factorization*, J. Complexity **23** (2007), no. 3, 380–420. MR MR2330992
- [6] Akpodigha Filatei, Xin Li, Marc Moreno Maza, and Éric Schost, *Implementation techniques for fast polynomial arithmetic in a high-level programming environment*, ISSAC ’06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 2006, pp. 93–100.
- [7] Katharina Geißler and Jürgen Klüners, *Galois group computation for rational polynomials*, J. Symbolic Comput. **30** (2000), no. 6, 653–674, Algorithmic methods in Galois theory. MR MR1800032 (2001k:12006)
- [8] Kiran S. Kedlaya, *Search techniques for root-unitary polynomials*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 71–81. MR MR2459990 (2009h:26022)
- [9] Sara Khodadad and Michael Monagan, *Fast rational function reconstruction*, ISSAC 2006, ACM, New York, 2006, pp. 184–190. MR MR2289118

- [10] Grégoire Lecerf, *New recombination algorithms for bivariate polynomial factorization based on Hensel lifting*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 2, 151–176. MR 2600710
- [11] Hsin-Chao Liao and Richard J. Fateman, *Evaluation of the heuristic polynomial GCD*, ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ACM Press, 1995, pp. 240–247.
- [12] Michael Monagan, *Maximal quotient rational reconstruction: An almost optimal algorithm for rational reconstruction*, ISSAC 2004, ACM, New York, 2004, pp. 243–249. MR MR2126950 (2005j:68137)
- [13] Jörn Müller-Quade and Rainer Steinwandt, *Basic algorithms for rational function fields*, J. Symbolic Comput. **27** (1999), no. 2, 143–170. MR MR1672124 (2000a:13043)
- [14] ———, *Gröbner bases applied to finitely generated field extensions*, J. Symbolic Comput. **30** (2000), no. 4, 469–490. MR MR1784753 (2001i:13040)
- [15] Fatima K. Abu Salem and Rawan N. Soudah, *An empirical study of cache-oblivious polygon indecomposability testing*, Computing **88** (2010), no. 8, 55–78.
- [16] Leonard Soicher and John McKay, *Computing Galois groups over the rationals*, J. Number Theory **20** (1985), no. 3, 273–281. MR MR797178 (87a:12002)
- [17] Allan Steel, *A new scheme for computing with algebraically closed fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 491–505. MR MR2041106 (2005b:12016)
- [18] Allan K. Steel, *Computing with algebraically closed fields*, J. Symbolic Comput. **45** (2010), no. 3, 342–372.
- [19] Rainer Steinwandt, *On computing a separating transcendence basis*, SIGSAM Bulletin **34** (2000), no. 4.

# Geometry

## Incidence Geometry

51Axx, 51Bxx

- [1] Jaume Agudé, *Four lines in space*, J. Geom. **92** (2009), no. 1-2, 1–16. MR MR2481514 (2010d:51002)
- [2] R. D. Baker and G. L. Ebert, *Construction of two-dimensional flag-transitive planes*, Geom. Dedicata **27** (1988), no. 1, 9–14. MR MR950320 (89f:51017)
- [3] ———, *Nests of size  $q - 1$  and another family of translation planes*, J. London Math. Soc. (2) **38** (1988), no. 2, 341–355. MR MR966305 (89k:51003)
- [4] ———, *A new class of translation planes*, Combinatorics '86 (Trento, 1986), Ann. Discrete Math., vol. 37, North-Holland, Amsterdam, 1988, pp. 7–20. MR MR931300 (89d:51010)
- [5] ———, *Filling the nest gaps*, Finite Fields Appl. **2** (1996), no. 1, 42–61. MR MR1371719 (97a:51015)
- [6] R. D. Baker, G. L. Ebert, and K. L. Wantz, *Regular hyperbolic fibrations*, Adv. Geom. **1** (2001), no. 2, 119–144. MR MR1840217 (2002f:51018)
- [7] R. D. Baker, G. L. Ebert, and R. Weida, *Another look at Bruen chains*, J. Combin. Theory Ser. A **48** (1988), no. 1, 77–90. MR MR938859 (89c:51002)
- [8] Simeon Ball, Gary Ebert, and Michel Lavrauw, *A geometric construction of finite semifields*, J. Algebra **311** (2007), no. 1, 117–129. MR MR2309880
- [9] F. Buekenhout and D. Leemans, *On apartments in incidence geometry*, 2009, p. 17.
- [10] Francis Buekenhout, Michel Dehon, and Isabelle De Schutter, *Projective injections of geometries and their affine extensions*, J. Geom. **52** (1995), no. 1-2, 41–53. MR MR1317254 (95m:51009)
- [11] Alan R. Camina and Federica Spiezia, *Sporadic groups and automorphisms of linear spaces*, J. Combin. Des. **8** (2000), no. 5, 353–362. MR MR1775788 (2001g:51012)

- [12] I. Cardinali, N. Durante, T. Penttila, and R. Trombetti, *Bruen chains over fields of small order*, Discrete Math. **282** (2004), no. 1-3, 245–247. MR MR2059524 (2004m:51008)
- [13] A. Cossidente, G. L. Ebert, and G. Korchmáros, *Unitals in finite Desarguesian planes*, J. Algebraic Combin. **14** (2001), no. 2, 119–125. MR MR1867228 (2002k:51010)
- [14] A. Cossidente, G. L. Ebert, G. Marino, and A. Siciliano, *Shult sets and translation ovoids of the Hermitian surface*, Adv. Geom. **6** (2006), no. 4, 523–542. MR MR2267036 (2007j:51009)
- [15] Craig Culbert and Gary L. Ebert, *Circle geometry and three-dimensional subregular translation planes*, Innov. Incidence Geom. **1** (2005), 3–18. MR MR2213951 (2006k:51003)
- [16] G. L. Ebert, *Spreads admitting regular elliptic covers*, European J. Combin. **10** (1989), no. 4, 319–330. MR MR1005838 (90i:51013)
- [17] ———, *Inverse planes with a given collection of common blocks*, Discrete Math. **131** (1994), no. 1-3, 81–90. MR MR1287723 (95j:51017)
- [18] G. L. Ebert and J. W. P. Hirschfeld, *Complete systems of lines on a Hermitian surface over a finite field*, Des. Codes Cryptogr. **17** (1999), no. 1-3, 253–268. MR MR1715266 (2000m:51006)
- [19] Norman L. Johnson and Keith E. Mellinger, *Multiple spread retraction*, Adv. Geom. **3** (2003), no. 3, 263–286. MR MR1997408 (2004j:51007)
- [20] J. D. Key and N. K. A. Rostom, *A characterisation of some finite inversive planes*, Ars Combin. **27** (1989), 193–195. MR MR989436 (90c:51009)
- [21] Dimitri Leemans, *Residually weakly primitive and locally two-transitive geometries for sporadic groups*, Mémoires de la Classe des Sciences, vol. 3, Académie royale de Belgique, 2008.
- [22] Dimitri Leemans and Laurence Vauthier, *An atlas of abstract regular polytopes for small groups*, Aequationes Math. **72** (2006), no. 3, 313–320. MR MR2282877

# Finite Geometry

51Exx

- [1] A. Aguglia, A. Cossidente, and G. L. Ebert, *Complete spans on Hermitian varieties*, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 7–15. MR MR1993152 (2004g:51006)
- [2] E. F. Assmus, Jr., *The coding theory of finite geometries and designs*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Rome, 1988), Lecture Notes in Comput. Sci., vol. 357, Springer, Berlin, 1989, pp. 1–6. MR MR1008488 (90f:51010)
- [3] E. F. Assmus, Jr. and J. D. Key, *Arcs and ovals in the Hermitian and Ree unitals*, European J. Combin. **10** (1989), no. 4, 297–308. MR MR1005835 (90g:51012)
- [4] ———, *Affine and projective planes*, Discrete Math. **83** (1990), no. 2-3, 161–187. MR MR1065696 (92e:51017a)
- [5] ———, *Baer subplanes, ovals and unitals*, Coding Theory and Design Theory, Part I, IMA Vol. Math. Appl., vol. 20, Springer, New York, 1990, pp. 1–8. MR MR1047867 (92e:51016)
- [6] ———, *Translation planes and derivation sets*, J. Geom. **37** (1990), no. 1-2, 3–16. MR MR1041974 (92e:51018a)
- [7] ———, *Correction: “Translation planes and derivation sets”*, J. Geom. **40** (1991), no. 1-2, 198. MR MR1102824 (92e:51018b)
- [8] ———, *Polynomial codes and finite geometries*, Handbook of Coding Theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1269–1343. MR MR1667952
- [9] Laura Bader, Nicola Durante, Maska Law, Guglielmo Lunardon, and Tim Penttila, *Symmetries of BLT-sets*, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 41–50. MR MR1993155 (2004f:51016)
- [10] Laura Bader, Christine M. O’Keefe, and Tim Penttila, *Some remarks on flocks*, J. Aust. Math. Soc. **76** (2004), no. 3, 329–343. MR MR2053507 (2005b:51008)
- [11] R. D. Baker, A. Bonisoli, A. Cossidente, and G. L. Ebert, *Mixed partitions of  $PG(5, q)$* , Discrete Math. **208/209** (1999), 23–29. MR MR1725517 (2000h:51018)

- [12] R. D. Baker, J. M. N. Brown, G. L. Ebert, and J. C. Fisher, *Projective bundles*, Bull. Belg. Math. Soc. Simon Stevin **1** (1994), no. 3, 329–336, A tribute to J. A. Thas (Gent, 1994). MR MR1317131 (96b:51009)
- [13] R. D. Baker, J. M. Dover, G. L. Ebert, and K. L. Wantz, *Hyperbolic fibrations of  $PG(3, q)$* , European J. Combin. **20** (1999), no. 1, 1–16. MR MR1669584 (2000d:51017)
- [14] ———, *Perfect Baer subplane partitions and three-dimensional flag-transitive planes*, Des. Codes Cryptogr. **21** (2000), no. 1-3, 19–39. MR MR1801160 (2002a:51010)
- [15] R. D. Baker and G. L. Ebert, *Construction of two-dimensional flag-transitive planes*, Geom. Dedicata **27** (1988), no. 1, 9–14. MR MR950320 (89f:51017)
- [16] ———, *Nests of size  $q-1$  and another family of translation planes*, J. London Math. Soc. (2) **38** (1988), no. 2, 341–355. MR MR966305 (89k:51003)
- [17] ———, *A new class of translation planes*, Combinatorics '86 (Trento, 1986), Ann. Discrete Math., vol. 37, North-Holland, Amsterdam, 1988, pp. 7–20. MR MR931300 (89d:51010)
- [18] ———, *Intersection of unitals in the Desarguesian plane*, Proceedings of the Twentieth Southeastern Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1989), vol. 70, 1990, pp. 87–94. MR MR1041587 (91b:51014)
- [19] ———, *On Buekenhout-Metz unitals of odd order*, J. Combin. Theory Ser. A **60** (1992), no. 1, 67–84. MR MR1156648 (93g:51009)
- [20] ———, *A Bruen chain for  $q = 19$* , Des. Codes Cryptogr. **4** (1994), no. 4, 307–312. MR MR1290615 (95h:51021)
- [21] ———, *Filling the nest gaps*, Finite Fields Appl. **2** (1996), no. 1, 42–61. MR MR1371719 (97a:51015)
- [22] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang, *A trace conjecture and flag-transitive affine planes*, J. Combin. Theory Ser. A **95** (2001), no. 1, 158–168. MR MR1840482 (2002c:11166)
- [23] R. D. Baker, G. L. Ebert, and K. L. Wantz, *Regular hyperbolic fibrations*, Adv. Geom. **1** (2001), no. 2, 119–144. MR MR1840217 (2002f:51018)



- [24] ———, *Enumeration of orthogonal Buekenhout unitals*, Des. Codes Cryptogr. **55** (2010), no. 2-3, 261–283. MR 2608432
- [25] R. D. Baker and K. L. Wantz, *Unitals in the code of the Hughes plane*, J. Combin. Des. **12** (2004), no. 1, 35–38. MR MR2024247 (2004j:94030)
- [26] Ronald D. Baker, C. Culbert, Gary L. Ebert, and Keith E. Mellinger, *Odd order flag-transitive affine planes of dimension three over their kernel*, Adv. Geom. **3** (2003), S215–S223, Special issue dedicated to Adriano Barlotti. MR MR2028398 (2005a:51009)
- [27] Ronald D. Baker, Jeremy M. Dover, Gary L. Ebert, and Kenneth L. Wantz, *Baer subgeometry partitions*, J. Geom. **67** (2000), no. 1-2, 23–34, Second Pythagorean Conference (Pythagoreion, 1999). MR MR1759706 (2001g:51010)
- [28] Simeon Ball, Gary Ebert, and Michel Lavrauw, *A geometric construction of finite semifields*, J. Algebra **311** (2007), no. 1, 117–129. MR MR2309880
- [29] John Bamberg and Tim Penttila, *A classification of transitive ovoids, spreads, and  $m$ -systems of polar spaces*, Forum Math. **21** (2009), no. 2, 181–216. MR MR2503303
- [30] L. M. Batten and J. M. Dover, *Some sets of type  $(m, n)$  in cubic order planes*, Des. Codes Cryptogr. **16** (1999), no. 3, 211–213. MR MR1689577 (2000d:51011)
- [31] Lynn M. Batten and Jeremy M. Dover, *Blocking semiovals of type  $(1, M + 1, N + 1)$* , SIAM J. Discrete Math. **14** (2001), no. 4, 446–457 (electronic). MR MR1861787 (2002h:51006)
- [32] O. Bauduin, *Géométries résiduellement faiblement primitives de petits groupes affins*, Diplomarbeit, Université Libre de Bruxelles, 1999.
- [33] Denis Bonheure, Francis Buekenhout, and Dimitri Leemans, *On the Petrials of thin rank 3 geometries*, J. Geom. **71** (2001), no. 1-2, 19–25. MR MR1848308 (2002g:51014)
- [34] A. Bonisoli and A. Cossidente, *Inscribed bundles, Veronese surfaces and caps*, Geometry, Combinatorial Designs and Related Structures (Spetses, 1996), London Math. Soc. Lecture Note Ser., vol. 245, Cambridge Univ. Press, Cambridge, 1997, pp. 27–32. MR MR1700837 (2000e:51014)
- [35] Arrigo Bonisoli and Antonio Cossidente, *Mixed partitions of projective geometries*, Des. Codes Cryptogr. **20** (2000), no. 2, 143–154. MR MR1774120 (2001d:51011)

- [36] Arrigo Bonisoli and Gloria Rinaldi, *A class of complete arcs in multiply derived planes*, Adv. Geom. (2003), no. suppl., S113–S118, Special issue dedicated to Adriano Barlotti. MR MR2028391 (2005d:51013)
- [37] F. Buekenhout, P. O. Dehaye, and D. Leemans, *RWPRI and  $(2T)_1$  flag-transitive linear spaces*, Beiträge Algebra Geom. **44** (2003), no. 1, 25–46. MR MR1990982 (2004j:51008)
- [38] F. Buekenhout and M. Hermand, *On flag-transitive geometries and groups*, Travaux de Mathématiques de l'Université Libre de Bruxelles **1** (1991), 45–78.
- [39] Francis Buekenhout, *Finite groups and geometries: A view on the present state and on the future*, Groups of Lie Type and their Geometries (Como, 1993), London Math. Soc. Lecture Note Ser., vol. 207, Cambridge Univ. Press, Cambridge, 1995, pp. 35–42. MR MR1320513 (96a:51006)
- [40] Francis Buekenhout, *All geometries for the smallest sporadic groups*, Tech. report, 2005.
- [41] Francis Buekenhout, Philippe Cara, Michel Dehon, and Dimitri Leemans, *Residually weakly primitive geometries of small sporadic and almost simple groups: a synthesis*, Topics in Diagram Geometry, Quad. Mat., vol. 12, Dept. Math., Seconda Univ. Napoli, Caserta, 2003, pp. 1–27. MR MR2066521 (2005e:51015)
- [42] Francis Buekenhout, Philippe Cara, and Koen Vanmeerbeek, *Geometries of the group  $\text{PSL}(2, 11)$* , Geom. Dedicata **83** (2000), no. 1-3, 169–206, Special issue dedicated to Helmut R. Salzmann on the occasion of his 70th birthday. MR MR1800018 (2001m:51017)
- [43] Francis Buekenhout, Michel Dehon, and Philippe Cara, *Geometries of small almost simple groups based on maximal subgroups*, Bull. Belg. Math. Soc. Simon Stevin (1998), no. suppl., ii+128. MR MR1620723 (99c:51017)
- [44] Francis Buekenhout, Michel Dehon, and Isabelle De Schutter, *Projective injections of geometries and their affine extensions*, J. Geom. **52** (1995), no. 1-2, 41–53. MR MR1317254 (95m:51009)
- [45] Francis Buekenhout, Michel Dehon, and Dimitri Leemans, *All geometries of the Mathieu group  $M_{11}$  based on maximal subgroups*, Experiment. Math. **5** (1996), no. 2, 101–110. MR MR1418957 (97h:51015)

- [46] ———, *On flag-transitive incidence geometries of rank 6 for the Mathieu group  $M_{12}$* , Groups and geometries (Siena, 1996), Trends Math., Birkhäuser, Basel, 1998, pp. 39–54. MR MR1644974 (99m:51017)
- [47] ———, *An atlas of residually weakly primitive geometries for small groups*, Acad. Roy. Belg. Cl. Sci. Mém. Collect. 8° (3) **14** (1999), 175. MR MR1833083 (2002c:05043)
- [48] Francis Buekenhout and Dimitri Leemans, *On a geometry of Ivanov and Shpectorov for the O’Nan sporadic simple group*, J. Combin. Theory Ser. A **85** (1999), no. 2, 148–164. MR MR1673924 (2000a:51014)
- [49] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *A group-theoretic framework for the construction of packings in Grassmannian spaces*, J. Algebraic Combin. **9** (1999), no. 2, 129–140. MR MR1679247 (2000e:51015)
- [50] Philippe Cara, *Exotische meetkunden van rang twee*, Dissertation, Universite Libre De Bruxelles, 1994.
- [51] Philippe Cara, *An infinite family of Petersen geometries with nonlinear diagram*, J. Geom. **67** (2000), no. 1-2, 73–88, Second Pythagorean Conference (Pythagoreion, 1999). MR MR1759711 (2001g:51011)
- [52] ———, *RWPRI geometries for the alternating group  $A_8$* , Finite Geometries, Dev. Math., vol. 3, Kluwer Acad. Publ., Dordrecht, 2001, pp. 61–97. MR MR2060757 (2005a:51019)
- [53] Philippe Cara and Dimitri Leemans, *The residually weakly primitive geometries of  $S_5 \times 2$* , Discrete Math. **255** (2002), no. 1-3, 35–45, Combinatorics ’98 (Palermo). MR MR1927781 (2003i:51012)
- [54] Philippe Cara, Serge Lehman, and Dmitrii V. Pasechnik, *On the number of inductively minimal geometries*, Theoret. Comput. Sci. **263** (2001), no. 1-2, 31–35, Combinatorics and computer science (Palaiseau, 1997). MR MR1846914 (2002e:05010)
- [55] A. Cossidente, *Caps embedded in the Klein quadric*, Bull. Belg. Math. Soc. Simon Stevin **7** (2000), no. 1, 13–19. MR MR1741740 (2001b:51017)
- [56] A. Cossidente, C. Culbert, G. L. Ebert, and G. Marino, *On  $m$ -ovoids of  $W_3(q)$* , Finite Fields Appl. **14** (2008), no. 1, 76–84. MR MR2381478

- [57] A. Cossidente, G. L. Ebert, and G. Korchmáros, *Unitals in finite Desarguesian planes*, J. Algebraic Combin. **14** (2001), no. 2, 119–125. MR MR1867228 (2002k:51010)
- [58] A. Cossidente, G. L. Ebert, G. Marino, and A. Siciliano, *Shult sets and translation ovoids of the Hermitian surface*, Adv. Geom. **6** (2006), no. 4, 523–542. MR MR2267036 (2007j:51009)
- [59] Antonio Cossidente and Marialuisa J. de Resmini, *The transitive and co-transitive blocking sets in  $\mathbf{P}^2(F_q)$* , Contrib. Discrete Math. **3** (2008), no. 1, 47–51. MR MR2375515
- [60] Antonio Cossidente, Gary L. Ebert, and Giuseppe Marino, *A complete span of  $H(4, 4)$  admitting  $\mathrm{PSL}_2(11)$  and related structures*, Contrib. Discrete Math. **3** (2008), no. 1, 52–57. MR MR2375516
- [61] Antonio Cossidente and Tim Penttila, *Hemisystems on the Hermitian surface*, J. London Math. Soc. (2) **72** (2005), no. 3, 731–741. MR MR2190334
- [62] ———, *On  $m$ -regular systems on  $H(5, q^2)$* , J. Algebraic Combin. **29** (2009), no. 4, 437–445. MR MR2506715
- [63] Antonio Cossidente and Angelo Sonnino, *Finite geometry and the Gale transform*, Discrete Math. **310** (2010), no. 22, 3206–3210. MR 2684091
- [64] Antonio Cossidente and Sam K. J. Vereecke, *Some geometry of the isomorphism  $\mathrm{Sp}(4, q) \cong \mathrm{O}(5, q)$ ,  $q$  even*, J. Geom. **70** (2001), no. 1-2, 28–37. MR MR1825542 (2002g:05043)
- [65] Patricia Vanden Cruyce, *Géométries des groupes  $\mathrm{PSL}(2, q)$* , Ph.D. thesis, Université Libre de Bruxelles, 1985.
- [66] Alexander A. Davydov, Giorgio Faina, Stefano Marcugini, and Fernanda Pambianco, *Computer search in projective planes for the sizes of complete arcs*, J. Geom. **82** (2005), no. 1-2, 50–62. MR MR2161814 (2006d:51009)
- [67] Michel Dehon, *Classifying geometries with Cayley*, J. Symbolic Comput. **17** (1994), no. 3, 259–276. MR MR1287332 (95f:51007)

- [68] Michel Dehon and Dimitri Leemans, *Constructing coset geometries with Magma: An application to the sporadic groups  $M_{12}$  and  $J_1$* , Atti Sem. Mat. Fis. Univ. Modena **50** (2002), no. 2, 415–427. MR MR1958289 (2003m:51016)
- [69] Alice Devillers, *Classification of Some Homogenous and Ultrahomogenous Structures*, Dissertation, Université Libre de Bruxelles, 2002.
- [70] ———, *A classification of finite partial linear spaces with a primitive rank 3 automorphism group of almost simple type*, Innov. Incidence Geom. **2** (2005), 129–175. MR MR2214719 (2007a:51012)
- [71] Cunsheng Ding, Zeying Wang, and Qing Xiang, *Skew Hadamard difference sets from the Ree-Tits slice symplectic spreads in  $PG(3, 3^{2h+1})$* , J. Combin. Theory Ser. A **114** (2007), no. 5, 867–887. MR MR2333138
- [72] Jeremy Dover, *Subregular spreads of  $PG(2n + 1, q)$* , Finite Fields Appl. **4** (1998), no. 4, 362–380. MR MR1648569 (99i:51010)
- [73] Jeremy M. Dover, *Semiovals with large collinear subsets*, J. Geom. **69** (2000), no. 1-2, 58–67. MR MR1800457 (2001k:51012)
- [74] ———, *Subregular spreads of  $PG(5, 2^e)$* , Finite Fields Appl. **7** (2001), no. 3, 421–427. MR MR1841907 (2002g:51010)
- [75] Sean V. Droms, Keith E. Mellinger, and Chris Meyer, *LDPC codes generated by conics in the classical projective plane*, Des. Codes Cryptogr. **40** (2006), no. 3, 343–356. MR MR2251325 (2007f:51021)
- [76] G. L. Ebert, *Spreads admitting regular elliptic covers*, European J. Combin. **10** (1989), no. 4, 319–330. MR MR1005838 (90i:51013)
- [77] ———, *Inverse planes with a given collection of common blocks*, Discrete Math. **131** (1994), no. 1-3, 81–90. MR MR1287723 (95j:51017)
- [78] ———, *Buekenhout-Tits unitals*, J. Algebraic Combin. **6** (1997), no. 2, 133–140. MR MR1436531 (97m:51009)
- [79] ———, *Replaceable nests*, Mostly finite geometries (Iowa City, IA, 1996), Lecture Notes in Pure and Appl. Math., vol. 190, Dekker, New York, 1997, pp. 35–49. MR MR1463976 (98m:51007)

- [80] ———, *Constructions in finite geometry using computer algebra systems*, J. Symbolic Comput. **31** (2001), no. 1-2, 55–70, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806206 (2001k:51017)
- [81] G. L. Ebert and J. W. P. Hirschfeld, *Complete systems of lines on a Hermitian surface over a finite field*, Des. Codes Cryptogr. **17** (1999), no. 1-3, 253–268. MR MR1715266 (2000m:51006)
- [82] G. L. Ebert, K. Metsch, and T. Szönyi, *Caps embedded in Grassmannians*, Geom. Dedicata **70** (1998), no. 2, 181–196. MR MR1620750 (99c:51016)
- [83] M. Gailly, *Géométries des groupes  $\text{PSL}(3, q)$ ,  $q < 7$* , Diplomarbeit, Université Libre de Bruxelles, 2001.
- [84] Maya Gailly and Dimitri Leemans, *The residually weakly primitive geometries of  $\text{PSL}(3, q)$  with  $q < 8$* , Aequationes Math. **67** (2004), no. 1-2, 195–196. MR MR2049618 (2005a:51007)
- [85] Rohit Ghosh, *Incompleteness of the Giulietti-Ughi arc for large primes*, Discrete Math. **308** (2008), no. 17, 3824–3835. MR MR2418086
- [86] Massimo Giulietti, *Involuppi di  $k$ -archi in piani proiettivi sopra campi finiti e basi di Gröbner*, Rendiconti del Circolo Matematico di Palermo **48** (1999), no. 1, 191–200.
- [87] David G. Glynn, *Theorems of points and planes in three-dimensional projective space*, J. Aust. Math. Soc **88** (2010), 75–92.
- [88] Valérie Gobbe, *Etude de petits groupes et des geometries associees a l'aide de Cayley*, Dissertation, Universite Libre De Bruxelles, 1991.
- [89] N. A. Gordon, R. Shaw, and L. H. Soicher, *Classification of partial spreads in  $PG(4, 2)$* .
- [90] Neil A. Gordon, Guglielmo Lunardon, and Ron Shaw, *Linear sections of  $GL(4, 2)$* , Bull. Belg. Math. Soc. Simon Stevin **5** (1998), no. 2-3, 287–311, Finite geometry and combinatorics (Deinze, 1997). MR MR1630033 (99g:51008)
- [91] Harald Gottschalk and Dimitri Leemans, *The residually weakly primitive geometries of the Janko group  $J_1$* , Groups and Geometries (Siena, 1996), Trends Math., Birkhäuser, Basel, 1998, pp. 65–79. MR MR1644976 (99h:51014)

- [92] ———, *Geometries for the group  $\text{PSL}(3, 4)$* , European J. Combin. **24** (2003), no. 3, 267–291. MR MR1969582 (2004m:51031)
- [93] Gerhard Grams and Thomas Meixner, *Some results about flag transitive diagram geometries using coset enumeration*, Ars Combin. **36** (1993), 129–146. MR MR1246906 (94j:51015)
- [94] G. Havas, C. R. Leedham-Green, E. A. O’Brien, and M. C. Slattery, *Certain Roman and flock generalized quadrangles have nonisomorphic elation groups*, Adv. Geom. **6** (2006), no. 3, 389–395. MR MR2248258
- [95] George Havas, C. R. Leedham-Green, E. A. O’Brien, and Michael C. Slattery, *Computing with elation groups*, Finite Geometries, Groups, and Computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 95–102. MR MR2258003 (2007f:20003)
- [96] M. Hermand, *Géométries, langage Cayley et groupe de Hall-Janko*, Ph.D. thesis, Université Libre de Bruxelles, 1991.
- [97] Pascale Jacobs and Dimitri Leemans, *An algorithmic analysis of the intersection property*, LMS J. Comput. Math. **7** (2004), 284–299 (electronic). MR MR2118176 (2005j:51007)
- [98] Norman L. Johnson, Giuseppe Marino, Olga Polverino, and Rocco Trombetti, *On a generalization of cyclic semifields*, J. Algebraic Combin. **29** (2009), no. 1, 1–34. MR MR2470113 (2010e:12010)
- [99] Norman L. Johnson and Keith E. Mellinger, *Multiple spread retraction*, Adv. Geom. **3** (2003), no. 3, 263–286. MR MR1997408 (2004j:51007)
- [100] Golala Abdulla Kadir, *On the affine geometries of  $M_{24}$* , Ph.D. thesis, University of Birmingham, 1984.
- [101] J. D. Key, *Codes and finite geometries*, Proceedings of the Twenty-ninth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1998), vol. 131, 1998, pp. 85–99. MR MR1676476 (2000a:51011)
- [102] ———, *Some applications of Magma in designs and codes: Oval designs, Hermitian unitals and generalized Reed-Muller codes*, J. Symbolic Comput. **31** (2001), no. 1-2, 37–53, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806205 (2002d:94064)

- [103] J. D. Key and M. J. de Resmini, *Small sets of even type and codewords*, J. Geom. **61** (1998), no. 1-2, 83–104. MR MR1603821 (98k:51024)
- [104] J. D. Key, T. P. McDonough, and V. C. Mavron, *Partial permutation decoding for codes from affine geometry designs*, J. Geom. **88** (2008), no. 1-2, 101–109. MR MR2398478
- [105] ———, *An upper bound for the minimum weight of the dual codes of Desarguesian planes*, European J. Combin. **30** (2009), no. 1, 220–229. MR MR2460228
- [106] J. D. Key and P. Seneviratne, *Codes from the line graphs of complete multipartite graphs and PD-sets*, Discrete Math. **307** (2007), no. 17-18, 2217–2225. MR MR2340603
- [107] J. D. Key and V. D. Tonchev, *Computational results for the known biplanes of order 9*, Geometry, Combinatorial Designs and Related Structures (Spetses, 1996), London Math. Soc. Lecture Note Ser., vol. 245, Cambridge Univ. Press, Cambridge, 1997, pp. 113–122. MR MR1700843 (2000e:51023)
- [108] Jennifer D. Key and Kirsten Mackenzie, *An upper bound for the  $p$ -rank of a translation plane*, J. Combin. Theory Ser. A **56** (1991), no. 2, 297–302. MR MR1092855 (92a:51005)
- [109] Jennifer D. Key, Johannes Siemons, and Ascher Wagner, *Regular sets on the projective line*, J. Geom. **27** (1986), no. 2, 188–194. MR MR867795 (88b:51012)
- [110] Nayil Kilic, *On rank 2 geometries of the Mathieu group  $M_{23}$* , Taiwanese Journal of Mathematics **14** (2010), no. 2, 373–387.
- [111] ———, *On rank 2 geometries of the Mathieu group  $M_{24}$* , An. St. Univ. Ovidius Constanta **18** (2010), no. 2, 131–148.
- [112] Hans-Joachim Kroll and Rita Vincenti, *PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of  $PG(5, 2)$* , Discrete Math. **308** (2008), no. 2-3, 408–414. MR MR2378042 (2008j:94066)
- [113] Maska Law, *Flocks, generalised quadrangles and translation planes from BLT-sets*, Ph.D. thesis, University of Western Australia, 2003.



- [114] Maska Law and Tim Penttila, *Classification of flocks of the quadratic cone over fields of order at most 29*, Adv. Geom. **3** (2003), no. Special Issue, S232–S244, Special issue dedicated to Adriano Barlotti. MR MR2028400 (2004m:51022)
- [115] ———, *Construction of BLT-sets over small fields*, European J. Combin. **25** (2004), no. 1, 1–22. MR MR2031798 (2004m:51023)
- [116] D. Leemans, *The residually weakly primitive geometries of  $M_{24}$* , 2002.
- [117] Dimitri Leemans, *Contribution à l'élaboration d'un Atlas de géométries: Volumes I and II*, Licence in mathematics, Université Libre De Bruxelles, 1994.
- [118] Dimitri Leemans, *Classification of RWPRI Geometries for the Suzuki Simple Groups*, PhD thesis, Université Libre de Bruxelles, 1998.
- [119] ———, *The rank 2 geometries of the simple Suzuki groups  $Sz(q)$* , Beiträge Algebra Geom. **39** (1998), no. 1, 97–120. MR MR1614433 (99b:20030)
- [120] ———, *Thin geometries for the Suzuki simple group  $Sz(8)$* , Bull. Belg. Math. Soc. Simon Stevin **5** (1998), no. 2-3, 373–387, Finite geometry and combinatorics (Deinze, 1997). MR MR1630038 (99f:51021)
- [121] ———, *An atlas of regular thin geometries for small groups*, Math. Comp. **68** (1999), no. 228, 1631–1647. MR MR1654025 (99m:51018)
- [122] ———, *The rank 3 geometries of the simple Suzuki groups  $Sz(q)$* , Note Mat. **19** (1999), no. 1, 43–63 (2000). MR MR1809899 (2001m:51019)
- [123] ———, *The residually weakly primitive geometries of the Suzuki simple group  $Sz(8)$* , Groups St. Andrews 1997 in Bath, II, London Math. Soc. Lecture Note Ser., vol. 261, Cambridge Univ. Press, Cambridge, 1999, pp. 517–526. MR MR1676648 (2000h:51025)
- [124] ———, *The residually weakly primitive geometries of the dihedral groups*, Atti Sem. Mat. Fis. Univ. Modena **48** (2000), no. 1, 179–190. MR MR1767379 (2001e:05027)
- [125] ———, *The residually weakly primitive pre-geometries of the Suzuki simple groups*, Note Mat. **20** (2000/01), no. 1, 1–20. MR MR1885309 (2003b:51021)
- [126] ———, *On a rank five geometry of Meixner for the Mathieu group  $M_{12}$* , Geom. Dedicata **85** (2001), no. 1-3, 273–281. MR MR1845612 (2002f:51021)

- [127] ———, *Some rank five geometries related to the Mathieu group  $M_{23}$* , J. Combin. Theory Ser. A **95** (2001), no. 2, 365–372. MR MR1845148 (2002d:51011)
- [128] ———, *The residually weakly primitive geometries of  $J_2$* , Note Mat. **21** (2002), no. 1, 77–81. MR MR1969351 (2004e:51012)
- [129] ———, *On a rank four geometry for the Hall-Janko sporadic group*, J. Combin. Theory Ser. A **101** (2003), no. 1, 160–167. MR MR1953287 (2004a:20023)
- [130] ———, *The residually weakly primitive geometries of  $M_{22}$* , Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 177–178. MR MR1993166 (2004f:51029)
- [131] ———, *Constructions of rank five geometries for the Mathieu group  $M_{22}$* , J. Geom. **79** (2004), no. 1-2, 146–155. MR MR2041690 (2005h:51011)
- [132] ———, *The residually weakly primitive geometries of  $J_3$* , Experiment. Math. **13** (2004), no. 4, 429–433. MR MR2118267 (2005i:51007)
- [133] ———, *The residually weakly primitive geometries of  $M_{23}$* , Atti Semin. Mat. Fis. Univ. Modena Reggio Emilia **52** (2004), no. 2, 313–316 (2005). MR MR2152818 (2006a:51011)
- [134] ———, *A generalization of a construction due to Van Nypelseer*, Beiträge Algebra Geom. **46** (2005), no. 2, 561–574. MR MR2196938
- [135] ———, *The residually weakly primitive geometries of  $HS$* , Australas. J. Combin. **33** (2005), 231–236. MR MR2170360
- [136] ———, *Two rank six geometries for the Higman-Sims sporadic group*, Discrete Math. **294** (2005), no. 1-2, 123–132. MR MR2139792 (2006i:51018)
- [137] Christiane Lefèvre-Percsy, Nicolas Percsy, and Dimitri Leemans, *New geometries for finite groups and polytopes*, Bull. Belg. Math. Soc. Simon Stevin **7** (2000), no. 4, 583–610. MR MR1806938 (2001m:51020)
- [138] Petr Lisoněk, Stefano Marcugini, and Fernanda Pambianco, *Constructions of small complete arcs with prescribed symmetry*, Contrib. Discrete Math. **3** (2008), no. 1, 14–19. MR MR2375512

- [139] S. Marcugini and F. Pambianco, *Minimal 1-saturating sets in  $PG(2, q)$ ,  $q \leq 16$* , Australas. J. Combin. **28** (2003), 161–169. MR MR1998870 (2004g:51010)
- [140] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco, *Classification of the  $(n, 3)$ -arcs in  $PG(2, 7)$* , J. Geom. **80** (2004), no. 1-2, 179–184. MR MR2176579
- [141] ———, *Maximal  $(n, 3)$ -arcs in  $PG(2, 13)$* , Discrete Math. **294** (2005), no. 1-2, 139–145. MR MR2139794 (2006a:51007)
- [142] ———, *Complete arcs in  $PG(2, 25)$ : the spectrum of the sizes and the classification of the smallest complete arcs*, Discrete Math. **307** (2007), no. 6, 739–747. MR MR2291449 (2007i:51014)
- [143] Justin McInroy and Sergey Shpectorov, *On the simple connectedness of hyperplane complements in dual polar spaces. II*, Discrete Math. **310** (2010), no. 8, 1381–1388. MR 2592492 (2011a:51004)
- [144] Keith E. Mellinger, *A note on line-Baer subspace partitions of  $PG(3, 4)$* , J. Geom. **72** (2001), no. 1-2, 128–131. MR MR1891460 (2003a:51013)
- [145] ———, *Designs, Geometry, and a Golfer's Dilemma*, Math. Mag. **77** (2004), no. 4, 275–282. MR MR1573761
- [146] Peter Müller and Gábor P. Nagy, *A note on the group of projectivities of finite projective planes*, Innov. Incidence Geom. **6/7** (2007/08), 291–294. MR MR2515272 (2010e:51009)
- [147] F. Pambianco and L. Storme, *Minimal blocking sets in  $PG(2, 9)$* , Ars Combin. **89** (2008), 223–234. MR MR2456247
- [148] Tim Penttila, *Applications of computer algebra to finite geometry*, Finite geometries, groups, and computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 203–221. MR MR2258011 (2007g:51007)
- [149] Tim Penttila and Blair Williams, *Ovoids of parabolic spaces*, Geom. Dedicata **82** (2000), no. 1-3, 1–19. MR MR1789057 (2001i:51005)
- [150] Olga Polverino, *Linear sets in finite projective spaces*, Discrete Math. **310** (2010), no. 22, 3096–3107.

- [151] B. B. Ranson and J. M. Dover, *Blocking semiovals in  $PG(2, 7)$  and beyond*, European J. Combin. **24** (2003), no. 2, 183–193. MR MR1961558 (2004d:51005)
- [152] Guyan Robertson, *Torsion in boundary coinvariants and  $K$ -theory for affine buildings*,  $K$ -Theory **33** (2005), no. 4, 347–369. MR MR2220525
- [153] Nagwa Kamal Ahmed Rostom, *Regular sets in incidence structures*, Ph.D. thesis, University of Birmingham, 1987.
- [154] M. Salazar-Neumann, *Rank 2 geometries of the group  $PSL(2, q)$* , 2000.
- [155] R. Shaw and N. A. Gordon, *The polynomial degree of the Grassmannian  $G_{1,n,2}$* , Des. Codes Cryptogr. **39** (2006), no. 2, 289–306. MR MR2209944 (2007a:51010)
- [156] Ron Shaw, *A property of  $A_7$ , and a maximal 3-dimensional linear section of  $GL(4, 2)$* , Discrete Math. **197/198** (1999), 733–747, 16th British Combinatorial Conference (London, 1997). MR MR1674900 (2000b:51007)
- [157] N. J. A. Sloane, *Packing planes in four dimensions and other mysteries*, In Algebraic Combinatorics and Related Topics (Yamagata 1997), ed. E. Bannai and M. Harada and M. Ozeki, Yamagata University, 1999. MR )
- [158] Kenneth L. Wantz, *Unitals embedded in finite projective planes*, PhD Thesis, University of Delaware, 1995.
- [159] Kenneth L. Wantz, *Unitals in the regular nearfield planes*, J. Geom. **88** (2008), no. 1-2, 169–177. MR MR2398487
- [160] Blair Williams, *Ovoids of Parabolic and Hyperbolic Spaces*, PhD Thesis, University of Western Australia, 1999.

# Real and Complex Geometry

51Mxx

- [1] Eiichi Bannai and Etsuko Bannai, *On Euclidean tight 4-designs*, J. Math. Soc. Japan **58** (2006), no. 3, 775–804. MR MR2254411
- [2] Ralph H. Buchholz and James A. MacDougall, *Cyclic polygons with rational sides and area*, J. Number Theory **128** (2008), no. 1, 17–48. MR MR2382768 (2008m:11061)
- [3] Marston Conder and Colin Maclachlan, *Compact hyperbolic 4-manifolds of small volume*, Proc. Amer. Math. Soc. **133** (2005), no. 8, 2469–2476 (electronic). MR MR2138890
- [4] Michael I. Hartley and Dimitri Leemans, *Quotients of a universal locally projective polytope of type  $\{5, 3, 5\}$* , Math. Z. **247** (2004), no. 4, 663–674. MR MR2077414 (2005c:51020)
- [5] Michael Ian Hartley and Dimitri Leemans, *On the thin regular geometries of rank four for the Janko group  $J_1$* , Innov. Incidence Geom. **1** (2005), 181–190. MR MR2213958 (2007d:51022)
- [6] Dimitri Leemans and Egon Schulte, *Groups of type  $L_2(q)$  acting on polytopes*, Adv. Geom. **7** (2007), no. 4, 529–539. MR MR2360900
- [7] Alen Orbanić, Daniel Pellicer, and Asia Ivić Weiss, *Map operations and  $k$ -orbit maps*, J. Combin. Theory Ser. A **117** (2010), no. 4, 411–429. MR 2592891 (2011a:51015)

# General Convexity

52Axx

- [1] Joseph H. G. Fu, *Structure of the unitary valuation algebra*, J. Differential Geom. **72** (2006), no. 3, 509–533. MR MR2219942 (2007b:52008)

# Polytopes and Polyhedra

52Bxx

- [1] Denis Bonheure, Francis Buekenhout, and Dimitri Leemans, *On the Petrials of thin rank 3 geometries*, J. Geom. **71** (2001), no. 1-2, 19–25. MR MR1848308 (2002g:51014)
- [2] Mireille Boutin and Gregor Kemper, *Which point configurations are determined by the distribution of their pairwise distances?*, Internat. J. Comput. Geom. Appl. **17** (2007), no. 1, 31–43. MR MR2296253
- [3] Marston Conder, *Combinatorial and computational group-theoretic methods in the study of graphs, maps and polytopes with maximal symmetry*, Jack Koolen and Jin Ho Kwak and Ming-Yao Xu, Eds. Applications of Group Theory to Combinatorics, Taylor & Francis Group, London, 2008, pp. 1–11.
- [4] Marston Conder, Isabel Hubard, and Tomaž Pisanski, *Constructions for chiral polytopes*, J. Lond. Math. Soc. (2) **77** (2008), no. 1, 115–129. MR MR2389920 (2009b:52031)
- [5] Joseph H. G. Fu, *Structure of the unitary valuation algebra*, J. Differential Geom. **72** (2006), no. 3, 509–533. MR MR2219942 (2007b:52008)
- [6] Michael I. Hartley, *Polytopes of finite type*, Discrete Math. **218** (2000), no. 1-3, 97–108. MR MR1754329 (2001f:52024)
- [7] Michael I. Hartley and Dimitri Leemans, *Quotients of a universal locally projective polytope of type  $\{5, 3, 5\}$* , Math. Z. **247** (2004), no. 4, 663–674. MR MR2077414 (2005c:51020)
- [8] ———, *A new Petrie-like construction for abstract polytopes*, J. Combin. Theory Ser. A **115** (2008), no. 6, 997–1007. MR MR2423344 (2009c:52024)
- [9] Isabel Hubard, Alen Orbanić, and Asia Ivić Weiss, *Monodromy groups and self-invariance*, Canad. J. Math. **61** (2009), no. 6, 1300–1324. MR MR2588424
- [10] Michael Joswig and Nikolaus Witte, *Products of foldable triangulations*, Adv. Math. **210** (2007), no. 2, 769–796. MR MR2303239 (2008c:52017)
- [11] John Little and Ryan Schwarz, *On  $m$ -dimensional toric codes*, 2005.

- [12] Peter Lorimer, *Four dodecahedral spaces*, Pacific J. Math. **156** (1992), no. 2, 329–335. MR MR1186809 (94a:57026)
- [13] Achill Schürmann and Frank Vallentin, *Computational approaches to lattice packing and covering problems*, Discrete Comput. Geom. **35** (2006), no. 1, 73–116. MR MR2183491 (2006k:52048)
- [14] L. Vauthier, *Atlas de polytopes réguliers issus de groupes presque simples*, Diplomarbeit, Université Libre de Bruxelles, 2005.



# Discrete Geometry

52Cxx

- [1] Mireille Boutin and Gregor Kemper, *On reconstructing  $n$ -point configurations from the distribution of distances or areas*, Adv. in Appl. Math. **32** (2004), no. 4, 709–735. MR MR2053842 (2005c:68259)
- [2] S. Allen Broughton, Robert M. Dirks, Maria T. Slougher, and C. Ryan Vinroot, *Triangular surface tiling groups for low genus*, 2001.
- [3] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin, *A generalization of Voronoi's reduction theory and its application*, Duke Math. J. **142** (2008), no. 1, 127–164. MR MR2397885 (2009a:11141)
- [4] Markus Grassl, *Computing equiangular lines in complex space*, Mathematical Methods in Computer Science, Lecture Notes in Comput. Sci., vol. 5393, 2008, pp. 89–104.
- [5] Michael Kiermaier and Sascha Kurz, *Maximal integral point sets in affine planes over finite fields*, Discrete Math. **309** (2009), no. 13, 4564–4575. MR MR2519195
- [6] Peter Lorimer, *Hyperbolic pyritohedra constructed from the Coxeter group  $[4, 3, 5]$* , Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 303–321. MR MR1344939 (96d:20037)
- [7] Achill Schürmann, *Perfect, strongly eutactic lattices are periodic extreme*, Adv. Math **225** (2010), no. 5, 2546–2564.
- [8] Achill Schürmann and Frank Vallentin, *Computational approaches to lattice packing and covering problems*, Discrete Comput. Geom. **35** (2006), no. 1, 73–116. MR MR2183491 (2006k:52048)
- [9] P. W. Shor and N. J. A. Sloane, *A family of optimal packings in Grassmannian manifolds*, J. Algebraic Combin. **7** (1998), no. 2, 157–163. MR MR1609881 (99b:52047)
- [10] N. J. A. Sloane, *Packing planes in four dimensions and other mysteries*, In Algebraic Combinatorics and Related Topics (Yamagata 1997), ed. E. Bannai and M. Harada and M. Ozeki, Yamagata University, 1999. MR )

- [11] N. J. A. Sloane, R. H. Hardin, T. D. S. Duff, and J. H. Conway, *Minimal-energy clusters of hard spheres*, *Discrete Comput. Geom.* **14** (1995), no. 3, 237–259. MR1344734 (96m:52033)

# Differential Geometry

53Xxx

- [1] Thomas Baird, *GKM sheaves and nonorientable surface group representations*, 2010.
- [2] Philip Boalch, *Some explicit solutions to the Riemann-Hilbert problem*, 2005.
- [3] Jennifer R. Daniel and Aloysius G. Helminck, *Computing the fine structure of real reductive symmetric spaces*, J. Symbolic Comput. **42** (2007), no. 5, 497–510. MR MR2322470
- [4] ———, *Algorithms for computations in local symmetric spaces*, Comm. Algebra **36** (2008), no. 5, 1758–1788. MR MR2424265
- [5] Bart de Smit, Ruth Gornet, and Craig J. Sutton, *Sunada’s method and the covering spectrum*, J. Differential Geom **To appear** (2011).
- [6] J. S. Dowker and Peter Chang, *Analytic torsion on spherical factors and tessellations*.
- [7] Joseph H. G. Fu, *Structure of the unitary valuation algebra*, J. Differential Geom. **72** (2006), no. 3, 509–533. MR MR2219942 (2007b:52008)
- [8] S. M. Salamon, *Complex structures on nilpotent Lie algebras*, J. Pure Appl. Algebra **157** (2001), no. 2-3, 311–333. MR MR1812058 (2002g:53089)

# Group Theory

## Permutation Groups

20Bxx

- [1] Edith Adan-Bante and Helena Verrill, *Symmetric groups and conjugacy classes*, J. Group Theory **11** (2008), no. 3, 371–379. MR MR2419007
- [2] C. Bates, D. Bundy, S. Hart, and P. Rowley, *A note on commuting graphs for symmetric groups*, Electron. J. Combin. **16** (2009), no. 1, 13. MR MR2475529
- [3] C. Bates, D. Bundy, Sarah B. Perkins, and P. Rowley, *Commuting involution graphs for symmetric groups*, J. Algebra **266** (2003), no. 1, 133–153. MR MR1994533 (2004h:20004)
- [4] Arrigo Bonisoli and Pasquale Quattrocchi, *Each invertible sharply  $d$ -transitive finite permutation set with  $d \geq 4$  is a group*, J. Algebraic Combin. **12** (2000), no. 3, 241–250. MR MR1803234 (2001m:20003)
- [5] Nigel Boston, Walter Dabrowski, Tuval Foguel, et al., *The proportion of fixed-point-free elements of a transitive permutation group*, Comm. Algebra **21** (1993), no. 9, 3259–3275. MR MR1228762 (94e:20002)
- [6] F. Buekenhout, A. Delandtsheer, and J. Doyen, *Finite linear spaces with flag-transitive groups*, J. Combin. Theory Ser. A **49** (1988), no. 2, 268–293. MR MR964388 (89k:20007)
- [7] Francis Buekenhout and Dimitri Leemans, *On the list of finite primitive permutation groups of degree  $\leq 50$* , J. Symbolic Comput. **22** (1996), no. 2, 215–225. MR MR1422147 (97g:20004)
- [8] David M. Bundy and Peter J. Rowley, *Symmetric groups and completions of the Goldschmidt amalgams of type  $G_1$* , J. Group Theory **9** (2006), no. 5, 627–640. MR MR2253956
- [9] Timothy C. Burness, Michael Giudici, and Robert A. Wilson, *Prime order derangements in primitive permutation groups*, 2010.

- [10] Greg Butler, *The transitive groups of degree fourteen and fifteen*, J. Symbolic Comput. **16** (1993), no. 5, 413–422. MR MR1271082 (95e:20006)
- [11] Peter J. Cameron, *Permutation Groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999. MR MR1721031 (2001c:20008)
- [12] ———, *Partitions and permutations*, Discrete Math. **291** (2005), no. 1-3, 45–54. MR MR2124054 (2005k:20003)
- [13] Peter J. Cameron, Michael Giudici, Gareth A. Jones, William M. Kantor, Mikhail H. Klin, Dragan Marušič, and Lewis A. Nowitz, *Transitive permutation groups without semiregular subgroups*, J. London Math. Soc. (2) **66** (2002), no. 2, 325–333. MR MR1920405 (2003f:20001)
- [14] A. R. Camina and L. Di Martino, *The group of automorphisms of a transitive 2-(91, 6, 1) design*, Geom. Dedicata **31** (1989), no. 2, 151–164. MR MR1012437 (91a:20006)
- [15] Alan R. Camina and Federica Spiezia, *Sporadic groups and automorphisms of linear spaces*, J. Combin. Des. **8** (2000), no. 5, 353–362. MR MR1775788 (2001g:51012)
- [16] John J. Cannon and Derek F. Holt, *The transitive permutation groups of degree 32*, Experiment. Math. **17** (2008), no. 3, 307–314. MR MR2455702
- [17] Marston Conder, *Generators for alternating and symmetric groups*, J. London Math. Soc. (2) **22** (1980), no. 1, 75–86. MR MR579811 (81h:20002)
- [18] ———, *More on generators for alternating and symmetric groups*, Quart. J. Math. Oxford Ser. (2) **32** (1981), no. 126, 137–163. MR MR615190 (82e:20001)
- [19] ———, *On the group of Rubik’s “magic” cube*, Bull. Inst. Math. Appl. **17** (1981), no. 11-12, 241–243. MR MR654751 (83e:20007)
- [20] ———, *The symmetric genus of alternating and symmetric groups*, J. Combin. Theory Ser. B **39** (1985), no. 2, 179–186. MR MR811121 (87e:20072)
- [21] ———, *Experimental algebra*, Math. Chronicle **20** (1991), 1–11. MR MR1137869 (92k:20007)
- [22] ———, *Generating the Mathieu groups and associated Steiner systems*, Discrete Math. **112** (1993), no. 1-3, 41–47. MR MR1213749 (94f:20004)

- [23] ———, *Group actions on graphs, maps and surfaces with maximum symmetry*, Groups St. Andrews 2001 in Oxford. Vol. I, London Math. Soc. Lecture Note Ser., vol. 304, Cambridge Univ. Press, Cambridge, 2003, pp. 63–91. MR MR2051519 (2004m:20005)
- [24] Marston Conder, *Combinatorial and computational group-theoretic methods in the study of graphs, maps and polytopes with maximal symmetry*, Jack Koolen and Jin Ho Kwak and Ming-Yao Xu, Eds. Applications of Group Theory to Combinatorics, Taylor & Francis Group, London, 2008, pp. 1–11.
- [25] Marston Conder and Vaughan Jones, *Highly transitive imprimitivities*, J. Algebra **300** (2006), no. 1, 44–56. MR MR2228633 (2007b:20008)
- [26] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular hypermaps over projective linear groups*, J. Aust. Math. Soc. **85** (2008).
- [27] John H. Conway, Alexander Hulpke, and John McKay, *On transitive permutation groups*, LMS J. Comput. Math. **1** (1998), 1–8 (electronic). MR MR1635715 (99g:20011)
- [28] Hannah J. Coutts, Martyn Quick, and Colva M. Roney-Dougal, *The primitive permutation groups of degree less than 4096*, 2010, pp. 1–23.
- [29] Robert T. Curtis, *A fresh approach to the exceptional automorphism and covers of the symmetric groups*, Arab. J. Sci. Eng. Sect. A Sci. **27** (2002), no. 1, 93–107. MR MR1878562 (2002j:20008)
- [30] A. Delgado and R. Weiss, *On certain coverings of generalized polygons*, Bull. London Math. Soc. **21** (1989), no. 3, 235–242. MR MR986364 (90b:20004)
- [31] Alice Devillers and Michael Giudici, *Involution graphs where the product of two adjacent vertices has order three*, J. Aust. Math. Soc. **85** (2008), no. 3, 305–322.
- [32] Ben Elias, Lior Silberman, and Ramin Takloo-Bighash, *Minimal permutation representations of nilpotent groups*, Experiment. Math. **19** (2010), no. 1, 121–128.
- [33] Ben Fairbairn, *Improved upper bounds on the spreads of some large sporadic groups*, 2009.
- [34] Derek F. Holt and Jacqueline Walton, *Representing the quotient groups of a finite permutation group*, J. Algebra **248** (2002), no. 1, 307–333. MR MR1879020 (2003b:20004)

- [35] Alexander Hulpke, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), no. 1, 1–30. MR MR2168238
- [36] William M. Kantor and Tim Penttala, *Reconstructing simple group actions*, Geometric Group Theory Down Under (Canberra, 1996), de Gruyter, Berlin, 1999, pp. 147–180. MR MR1714844 (2000h:20008)
- [37] Jennifer D. Key and Johannes Siemons, *Closure properties of the special linear groups*, Ars Combin. **22** (1986), 107–117. MR MR867739 (88a:20009)
- [38] ———, *On the  $k$ -closure of finite linear groups*, Boll. Un. Mat. Ital. B (7) **1** (1987), no. 1, 31–55. MR MR895449 (88g:20008)
- [39] Dimitri Leemans, *Two nearly isomorphic groups*, Atti Sem. Mat. Fis. Univ. Modena **45** (1997), no. 2, 373–376. MR MR1601985 (98k:20005)
- [40] Cai Heng Li, Zai Ping Lu, and Dragan Marušič, *On primitive permutation groups with small suborbits and their orbital graphs*, J. Algebra **279** (2004), no. 2, 749–770. MR MR2078940 (2005d:20003)
- [41] A. M. Macbeath, *Superimprimitive 2-generator finite groups*, Proc. Edinburgh Math. Soc. (2) **30** (1987), no. 1, 103–113, Groups—St. Andrews 1985. MR MR879436 (88d:20004)
- [42] Steve Medvedoff and Kent Morrison, *Groups of perfect shuffles*, Math. Mag. **60** (1987), no. 1, 3–14. MR MR876415 (88c:20007)
- [43] Torsten Minkwitz, *An algorithm for solving the factorization problem in permutation groups*, J. Symbolic Comput. **26** (1998), no. 1, 89–95. MR MR1633589 (99e:20004)
- [44] Alen Orbanić,  *$F$ -actions and parallel-product decomposition of reflexible maps*, J. Algebraic Combin. **26** (2007), no. 4, 507–527. MR MR2341863
- [45] Geoffrey Pearce, *Examples of rank 3 product action transitive decompositions*, Des. Codes Cryptogr. **47** (2008), no. 1-3, 289–303. MR MR2375474 (2008m:20004)
- [46] Wilhelm Plesken, *Counting with groups and rings*, J. Reine Angew. Math. **334** (1982), 40–68. MR MR667449 (84a:20008)
- [47] Cheryl E. Praeger and Leonard H. Soicher, *Low Rank Representations and Graphs for Sporadic Groups*, Australian Mathematical Society Lecture Series, vol. 8, Cambridge University Press, Cambridge, 1997. MR MR1430574 (97m:20006)

- [48] Colva M. Roney-Dougal, *The primitive permutation groups of degree less than 2500*, J. Algebra **292** (2005), no. 1, 154–183. MR MR2166801
- [49] Colva M. Roney-Dougal and William R. Unger, *The affine primitive permutation groups of degree less than 1000*, J. Symbolic Comput. **35** (2003), no. 4, 421–439. MR MR1976576 (2004e:20002)
- [50] Gordon F. Royle, *The transitive groups of degree twelve*, J. Symbolic Comput. **4** (1987), no. 2, 255–268. MR MR922391 (89b:20010)
- [51] Gordon F. Royle and Cheryl E. Praeger, *Constructing the vertex-transitive graphs of order 24*, J. Symbolic Comput. **8** (1989), no. 4, 309–326. MR MR1021609 (91a:68216)
- [52] Neil Saunders, *Minimal faithful permutation degrees for irreducible Coxeter groups*, 2008.
- [53] Ákos Seress, *Permutation Group Algorithms*, Cambridge Tracts in Mathematics, vol. 152, Cambridge University Press, Cambridge, 2003. MR MR1970241 (2004c:20008)
- [54] ———, *A unified approach to computations with permutation and matrix groups*, International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zürich, 2006, pp. 245–258. MR MR2275596 (2008a:20006)
- [55] John van Bon and Arjeh M. Cohen, *Linear groups and distance-transitive graphs*, European J. Combin. **10** (1989), no. 5, 399–411. MR MR1014547 (90h:20006)
- [56] Richard Weiss, *A characterization of the group  $\hat{M}_{12}$* , Proceedings of the Conference on Groups and Geometry, Part B (Madison, Wis., 1985), Algebras, Groups and Geometries, vol. 2,4, 1985, pp. 555–563. MR MR852424 (87k:20010)



# Representation Theory

20Cxx

- [1] A. Abduh and R. J. List, *The characters of the centralizer of an involution in  $C_1$* , Arch. Math. (Basel) **51** (1988), no. 6, 485–490. MR MR973721 (90b:20010)
- [2] Jaume Agué, *The arboreal approach to pairs of involutions in rank two*, Comm. Algebra **37** (2009), no. 3, 1104–1116. MR MR2503197
- [3] Faryad Ali and Jamshid Moori, *The Fischer-Clifford matrices of a maximal subgroup of  $\text{Fi}'_{24}$* , Represent. Theory **7** (2003), 300–321 (electronic). MR MR1993362 (2004i:20023)
- [4] ———, *Fischer-Clifford matrices of the non-split group extension  $2^6 \cdot U_4(2)$* , Quaest. Math. **31** (2008), no. 1, 27–36. MR MR2404644
- [5] Jianbei An, *Dade's conjecture for the Tits group*, New Zealand J. Math. **25** (1996), no. 2, 107–131. MR MR1421484 (97h:20009)
- [6] ———, *The Alperin and Dade conjectures for the simple Held group*, J. Algebra **189** (1997), no. 1, 34–57. MR MR1432364 (97k:20025)
- [7] Jianbei An, John J. Cannon, E. A. O'Brien, and W. R. Unger, *The Alperin weight conjecture and Dade's conjecture for the simple group  $\text{Fi}'_{24}$* , LMS J. Comput. Math. **11** (2008), 100–145. MR MR2410917
- [8] Jianbei An and Marston Conder, *The Alperin and Dade conjectures for the simple Mathieu groups*, Comm. Algebra **23** (1995), no. 8, 2797–2823. MR MR1332147 (96e:20013)
- [9] Jianbei An and E. A. O'Brien, *A local strategy to decide the Alperin and Dade conjectures*, J. Algebra **206** (1998), no. 1, 183–207. MR MR1637276 (99d:20015)
- [10] ———, *The Alperin and Dade conjectures for the Fischer simple group  $\text{Fi}_{23}$* , Internat. J. Algebra Comput. **9** (1999), no. 6, 621–670. MR MR1727163 (2001a:20026)
- [11] ———, *The Alperin and Dade conjectures for the O'Nan and Rudvalis simple groups*, Comm. Algebra **30** (2002), no. 3, 1305–1348. MR MR1892603 (2003a:20020)

- [12] ———, *Conjectures on the character degrees of the Harada-Norton simple group HN*, Israel J. Math. **137** (2003), 157–181. MR MR2013354 (2004k:20032)
- [13] ———, *The Alperin and Dade conjectures for the Conway simple group  $\text{Co}_1$* , Algebr. Represent. Theory **7** (2004), no. 2, 139–158. MR MR2063006 (2005g:20021)
- [14] ———, *The Alperin and Uno conjectures for the Fischer simple group  $\text{Fi}_{22}$* , Comm. Algebra **33** (2005), no. 5, 1529–1557. MR MR2149075 (2006c:20023)
- [15] Jianbei An, E. A. O’Brien, and R. A. Wilson, *The Alperin weight conjecture and Dade’s conjecture for the simple group  $J_4$* , LMS J. Comput. Math. **6** (2003), 119–140 (electronic). MR MR1998146 (2004h:20018)
- [16] Jianbei An and R. A. Wilson, *The Alperin weight conjecture and Uno’s conjecture for the Baby Monster  $B$ ,  $p$  odd*, LMS J. Comput. Math. **7** (2004), 120–166 (electronic). MR MR2087094 (2005g:20022)
- [17] Henrik Bäärnhielm, *Algorithmic problems in twisted groups of Lie type*, 2008.
- [18] Martina Balagovic and Arjun Puranik, *Irreducible representations of the rational Cherednik algebra associated to the Coxeter group  $H_3$* , 2010.
- [19] Ayala Bar-Ilan, Tzviya Berrebi, Genadi Chereshnya, Ruth Leabovich, Mikhal Cohen, and Mary Schaps, *Explicit tilting complexes for the Broué conjecture on 3-blocks*, vol. 1, Cambridge University Press, 2005.
- [20] R. W. Barraclough and R. A. Wilson, *The character table of a maximal subgroup of the Monster*, LMS J. Comput. Math. **10** (2007), 161–175 (electronic). MR MR2308856
- [21] B. Bekka, P. de la Harpe, and A. Valette, *Kazhdan’s Property (t)*, New Mathematical Monographs, no. 11, Cambridge University Press, Cambridge, 2008.
- [22] C. P. Bendel, D. K. Nakano, B. J. Parshall, and C. Pillen, *Cohomology for quantum groups via the geometry of the Nullcone*, 2007, pp. 1–58.
- [23] D. J. Benson and J. F. Carlson, *Cohomology of the double cover of the Mathieu group  $M_{12}$* , J. Algebra **226** (2000), no. 1, 547–576. MR MR1749904 (2001h:20076)
- [24] David J. Benson, Philip Bergonio, Brian D. Boe, Leonard Chastkofsky, Bobbe Cooper, Jeremiah Hower, Jo Jang Hyun, Jonathan Kujawa, Nadia Mazza, Daniel K.

- Nakano, Kenyon J. Platt, and Caroline Wright, *Support varieties for Weyl modules over bad primes*, *J. Algebra* **312** (2007), no. 2, 602–633.
- [25] Christine Bessenrodt, *Tensor products of representations of the symmetric groups and related groups*, *Sūrikaisekikenyūsho Kōkyūroku* (2000), no. 1149, 1–15, Representation theory of finite groups and related topics (Japanese) (Kyoto, 1998). MR MR1796358
- [26] Jonah Blasiak, *W-graph versions of tensoring with the  $S_n$  defining representation*, 2008.
- [27] J. D. Bradley and P. E. Holmes, *Improved bounds for the spread of sporadic groups*, *LMS J. Comput. Math.* **10** (2007), 132–140 (electronic). MR MR2308854 (2008b:20020)
- [28] John N. Bray and Robert T. Curtis, *Monomial modular representations and symmetric generation of the Harada-Norton group*, *J. Algebra* **268** (2003), no. 2, 723–743. MR MR2009330 (2005h:20023)
- [29] Peter A. Brooksbank and Eugene M. Luks, *Testing isomorphism of modules*, *J. Algebra* **320** (2008), no. 11, 4020–4029. MR MR2464805 (2009h:16001)
- [30] Peter A. Brooksbank and E. A. O’Brien, *Constructing the group preserving a system of forms*, *Internat. J. Algebra Comput.* **18** (2008), no. 2, 227–241. MR MR2403820
- [31] Jon F. Carlson, *Constructing endotrivial modules*, *J. Pure Appl. Algebra* **206** (2006), no. 1-2, 83–110. MR MR2220083 (2006m:20017)
- [32] ———, *Support varieties for modules*, *Discovering Mathematics with Magma, Algorithms Comput. Math.*, vol. 19, Springer, Berlin, 2006, pp. 187–204. MR MR2278928
- [33] ———, *When is projectivity detected on subalgebras?*, *Discovering Mathematics with Magma, Algorithms Comput. Math.*, vol. 19, Springer, Berlin, 2006, pp. 205–220. MR MR2278929
- [34] Jon F. Carlson, David J. Hemmer, and Nadia Mazza, *The group of endotrivial modules for the symmetric and alternating groups*, *Proc. Edinb. Math. Soc. (2)* **53** (2010), no. 1, 83–95. MR MR2579680

- [35] Jon F. Carlson, Nadia Mazza, and Daniel K. Nakano, *Endotrivial modules for finite groups of Lie type*, J. Reine Angew. Math. **595** (2006), 93–119. MR MR2244799 (2007c:20023)
- [36] ———, *Endotrivial modules for the symmetric and alternating groups*, Proc. Edinb. Math. Soc. (2) **52** (2009), 45–66. MR MR2475880 (2009k:20023)
- [37] Jon F. Carlson and Jacques Thévenaz, *Torsion endo-trivial modules*, Algebr. Represent. Theory **3** (2000), no. 4, 303–335, Special issue dedicated to Klaus Roggenkamp on the occasion of his 60th birthday. MR MR1808129 (2001m:20014)
- [38] ———, *The classification of endo-trivial modules*, Invent. Math. **158** (2004), no. 2, 389–411. MR MR2096798 (2005e:20013)
- [39] ———, *The classification of torsion endo-trivial modules*, Ann. of Math. (2) **162** (2005), no. 2, 823–883. MR MR2183283 (2006f:20012)
- [40] Marston Conder, C. R. Leedham-Green, and E. A. O’Brien, *Constructive recognition of  $\mathrm{PSL}(2, q)$* , Trans. Amer. Math. Soc. **358** (2006), no. 3, 1203–1221 (electronic). MR MR2187651 (2006j:20017)
- [41] Adán Cortés-Medina and Luis Valero-Elizondo, *A computational verification of Alperin’s weight conjecture for groups of small order and their prime fields*, Rev. Colomb. Mat. **41** (2007), no. 2, 325–331.
- [42] David A. Craven, *Simple modules for groups with abelian Sylow 2-subgroups are algebraic*, J. Algebra **321** (2009), no. 5, 1473–1479. MR MR2494402
- [43] Susanne Danz, *On vertices of exterior powers of the natural simple module for the symmetric group in odd characteristic*, Arch. Math. (Basel) **89** (2007), no. 6, 485–496. MR MR2371684 (2008i:20014)
- [44] ———, *Vertices of low-dimensional simple modules for symmetric groups*, Comm. Algebra **36** (2008), no. 12, 4521–4539. MR MR2473346 (2009j:20021)
- [45] ———, *On vertices of completely spittable modules for symmetric groups and simple modules labelled by two part partitions*, J. Group Theory **12** (2009), no. 3, 351–385. MR MR2510202
- [46] Susanne Danz and Karin Erdmann, *The vertices of a class of Specht modules and simple modules for symmetric groups in characteristic 2*, 2010, pp. 1–32.

- [47] Susanne Danz and Burkhard Külshammer, *The vertices and sources of the basic spin module for the symmetric group in characteristic 2*, J. Pure Appl. Algebra **213** (2009), no. 7, 1264–1282. MR MR2497574
- [48] ———, *Vertices of simple modules for symmetric groups: A survey*, Proceedings of the International Conference on Modules and Representation Theory, Presa Univ. Clujeană, Cluj-Napoca, 2009, pp. 61–77. MR MR2603204
- [49] ———, *Vertices, sources and Green correspondents of the simple modules for the large Mathieu groups*, J. Algebra **322** (2009), no. 11, 3919–3949. MR MR2556131
- [50] Susanne Danz, Burkhard Külshammer, and René Zimmermann, *On vertices of simple modules for symmetric groups of small degrees*, J. Algebra **320** (2008), no. 2, 680–707. MR MR2422312
- [51] Susanne Danz and René Zimmermann, *Vertices of simple modules for the symmetric groups in blocks of small weights*, Beiträge Algebra Geom. **49** (2008), no. 2, 409–427. MR MR2468066 (2009j:20020)
- [52] Willem A. de Graaf and Oksana S. Yakimova, *Good index behaviour of  $\theta$ -representations, i*, arXiv:1003.4162v1 (2010).
- [53] Harald Ellers and John Murray, *Branching rules for Specht modules*, J. Algebra **307** (2007), no. 1, 278–286. MR MR2278054 (2007k:20007)
- [54] Pavel Etingof, Frédéric Latour, and Eric Rains, *On central extensions of preprojective algebras*, J. Algebra **313** (2007), no. 1, 165–175. MR MR2326141
- [55] Pavel Etingof and Eric Rains, *Central extensions of preprojective algebras, the quantum Heisenberg algebra, and 2-dimensional complex reflection groups*, J. Algebra **299** (2006), no. 2, 570–588. MR MR2228327 (2007f:16037)
- [56] Claus Fieker, *Minimizing representations over number fields*, J. Symbolic Comput. **38** (2004), no. 1, 833–842. MR MR2094558 (2005g:20023)
- [57] ———, *Minimizing representations over number fields II. Computations in the Brauer group*, J. Algebra **322** (2009), no. 3, 752–765. MR MR2531221
- [58] Andrew Francis, *The minimal basis for the centre of an Iwahori-Hecke algebra*, J. Algebra **221** (1999), no. 1, 1–28. MR MR1722901 (2000k:20005)

- [59] S.P. Glasby and Cheryl E. Praeger, *Towards an efficient Meat-axe algorithm using  $f$ -cyclic matrices: The density of uncyclic matrices in  $M(n, q)$* , J. Algebra **322** (2009), no. 3, 766–790.
- [60] H. W. Gollan and T. W. Ostermann, *Operation of class sums on permutation modules*, J. Symbolic Comput. **9** (1990), no. 1, 39–47. MR MR1044913 (91a:20017)
- [61] Markus Grassl, *Constructing matrix representations of finite groups in characteristic zero*, Proceedings 10th Rhine Workshop on Computer Algebra (RWCA06, 2006, pp. 143–148.
- [62] David J. Green, *Gröbner bases for  $p$ -group algebras*, 2009.
- [63] Robert Guralnick and Susan Montgomery, *Frobenius-Schur indicators for subgroups and the Drinfeld double of Weyl groups*, Trans. Amer. Math. Soc. **361** (2009), no. 7, 3611–3632. MR MR2491893
- [64] David J. Hemmer, *The complexity of certain Specht modules for the symmetric group*, J. Algebraic Combin. **30** (2009), no. 4, 421–427. MR MR2563134
- [65] Stuart Hendren, *Extra special defect groups of order  $p^3$  and exponent  $p$* , J. Algebra **313** (2007), no. 2, 724–760. MR MR2329566
- [66] R. J. Higgs, *The bad behavior of representation groups*, J. Algebra Appl. **4** (2005), no. 2, 139–151. MR MR2139260 (2006b:20009)
- [67] R. J. Higgs and J. F. Humphreys, *Projective character degree patterns of 2-groups*, Comm. Algebra **28** (2000), no. 3, 1189–1210. MR MR1742650 (2001a:20020)
- [68] G. Hiss, *Algorithms of representation theory*, Computer Algebra Handbook (J. Grabmeier, E. Kaltofen, and V. Weispfenning, eds.), vol. 17, Springer, Berlin, 2003, pp. 84–88.
- [69] Miles Holloway, *Broué’s conjecture for the Hall-Janko group and its double cover*, Proc. London Math. Soc. (3) **86** (2003), no. 1, 109–130. MR MR1971465 (2004a:20020)
- [70] Miles Lee Holloway, *Derived equivalences for group algebras*, Dissertation, University of Bristol, 2001.

- [71] Derek F. Holt, C. R. Leedham-Green, E. A. O'Brien, and Sarah Rees, *Computing matrix group decompositions with respect to a normal subgroup*, J. Algebra **184** (1996), no. 3, 818–838. MR MR1407872 (97m:20021)
- [72] ———, *Testing matrix groups for primitivity*, J. Algebra **184** (1996), no. 3, 795–817. MR MR1407871 (97m:20020)
- [73] Derek F. Holt and Sarah Rees, *Testing modules for irreducibility*, J. Austral. Math. Soc. Ser. A **57** (1994), no. 1, 1–16. MR MR1279282 (95e:20023)
- [74] Shih-Chang Huang, *Uno's conjecture for the Chevalley simple groups  $G_2(3)$  and  $G_2(4)$* , New Zealand J. Math. **35** (2006), no. 2, 155–182. MR MR2325581
- [75] Stephen P. Humphries, *Some linear representations of braid groups*, J. Knot Theory Ramifications **9** (2000), no. 3, 341–366. MR MR1753799 (2001b:20011)
- [76] I. M. Isaacs, *Counting characters of upper triangular groups*, J. Algebra **315** (2007), no. 2, 698–719. MR MR2351888
- [77] I. M. Isaacs and Dikran Karagueuzian, *Conjugacy in groups of upper triangular matrices*, J. Algebra **202** (1998), no. 2, 704–711. MR MR1617655 (99b:20011)
- [78] ———, *Erratum: "Conjugacy in groups of upper triangular matrices" [*J. Algebra* **202** (1998), no. 2, 704–711; MR1617655 (99b:20011)]*, J. Algebra **208** (1998), no. 2, 722. MR MR1655475 (99g:20021)
- [79] I. M. Isaacs and Tom Wilde, *Primitive characters of maximal subgroups of solvable groups*, J. Algebra **323** (2010), no. 2, 419–436. MR MR2564848
- [80] Christoph Jansen, *The minimal degrees of faithful representations of the sporadic simple groups and their covering groups*, LMS J. Comput. Math. **8** (2005), 122–144 (electronic). MR MR2153793
- [81] D. Joyner, *Arithmetic of characters of generalized symmetric groups*, Arch. Math. (Basel) **81** (2003), no. 2, 113–120. MR MR2009553 (2004k:20019)
- [82] D. B. Karagueuzian and P. Symonds, *The module structure of a group action on a polynomial ring: Examples, generalizations, and applications*, Invariant Theory in all Characteristics, CRM Proc. Lecture Notes, vol. 35, Amer. Math. Soc., Providence, RI, 2004, pp. 139–158. MR MR2066462 (2005g:13011)

- [83] Dikran B. Karagueuzian and Peter Symonds, *The module structure of a group action on a polynomial ring*, J. Algebra **218** (1999), no. 2, 672–692. MR MR1705758 (2000f:20011)
- [84] ———, *The module structure of a group action on a polynomial ring: a finiteness theorem*, J. Amer. Math. Soc. **20** (2007), no. 4, 931–967 (electronic). MR MR2328711
- [85] Hyun Kyu Kim and Gerhard O. Michler, *Construction of  $Co_1$  from an irreducible subgroup  $M_{24}$  of  $GL_{11}(2)$* , 2009.
- [86] Markus Kirschmer, *Finite symplectic matrix groups*.
- [87] Joachim König, *Solvability of generalized monomial groups*, 2009.
- [88] L. G. Kovács and Ralph Stöhr, *Lie powers of the natural module for  $GL(2)$* , J. Algebra **229** (2000), no. 2, 435–462. MR MR1769283 (2001h:20070)
- [89] M. Kratzer, G. O. Michler, and M. Weller, *Harada group uniquely determined by centralizer of a 2-central involution*, Proceedings of the First Sino-German Workshop on Representation Theory and Finite Simple Groups (Beijing, 2002), vol. 10, 2003, pp. 303–372. MR MR2014018 (2004h:20020)
- [90] Mathias Kratzer, *Konkrete Charaktertafeln und kompatible Charaktere*, Vorlesungen aus dem Fachbereich Mathematik der Universität GH Essen [Lecture Notes in Mathematics at the University of Essen], vol. 30, Universität Essen Fachbereich Mathematik, Essen, 2001, Dissertation, Universität Essen, Essen, 2001. MR MR1864058 (2002j:20037)
- [91] ———, *Constructing pairs of compatible characters*, Proceedings of the First Sino-German Workshop on Representation Theory and Finite Simple Groups (Beijing, 2002), vol. 10, 2003, pp. 285–302. MR MR2014017 (2004h:20019)
- [92] Matthias Külzner, *On representations of twisted group rings*, J. Group Theory **7** (2004), no. 2, 197–229. MR MR2049017 (2005h:20004)
- [93] Matthias Külzner and Andrew Mathas, *Elementary divisors of Specht modules*, European J. Combin. **26** (2005), no. 6, 943–964. MR MR2143203 (2006a:20012)
- [94] Alain LeBel, D. L. Flannery, and K. J. Horadam, *Group algebra series and coboundary modules*, J. Pure Appl. Algebra **214** (2010), no. 7, 1291–1300. MR 2587004 (2011b:20011)



- [95] W. Lempken and R. Staszewski, *A construction of  $\widehat{3}\text{McL}$  and some representation theory in characteristic 5*, Linear Algebra Appl. **192** (1993), 205–234, Computational linear algebra in algebraic and related problems (Essen, 1992). MR MR1236744 (94k:20015)
- [96] ———, *Some 5-modular representation theory for the simple group  $\text{McL}$* , Comm. Algebra **21** (1993), no. 5, 1611–1629. MR MR1213977 (94a:20027)
- [97] ———, *The structure of the projective indecomposable modules of  $\widehat{3}M_{22}$  in characteristic 2*, Math. Comp. **62** (1994), no. 206, 841–850. MR MR1216260 (94g:20016)
- [98] Mark L. Lewis, *Generalizing a theorem of Huppert and Manz*, J. Algebra Appl. **6** (2007), no. 4, 687–695. MR MR2350989 (2008f:20018)
- [99] ———, *A group with three real irreducible characters: answering a question of Moretó and Navarro*, J. Algebra Appl. **8** (2009), no. 4, 453–459. MR MR2555513
- [100] ———, *The vanishing-off subgroup*, J. Algebra **321** (2009), no. 4, 1313–1325. MR MR2489902
- [101] Kay Jin Lim, *The varieties for some Specht modules*, J. Algebra **321** (2009), no. 8, 2287–2301. MR MR2501521
- [102] K. Lux and H. Pahlings, *Computational aspects of representation theory of finite groups*, Representation theory of finite groups and finite-dimensional algebras (Bielefeld, 1991), Progr. Math., vol. 95, Birkhäuser, Basel, 1991, pp. 37–64. MR MR1112157 (92g:20025)
- [103] Kay Magaard, E. A. O’Brien, and Ákos Seress, *Recognition of small dimensional representations of general linear groups*, J. Aust. Math. Soc. **85** (2008), no. 2, 229–250. MR MR2470540
- [104] Ivan Marin and Jean Michel, *Automorphisms of complex reflection groups*, 2007.
- [105] Conchita Martínez-Perez and Wolfgang Willems, *The trivial intersection problem for characters of principal indecomposable modules*, Adv. Math. **222** (2009), no. 4, 1197–1219.
- [106] Gerhard O. Michler, *Some problems in computational representation theory*, J. Symbolic Comput. **9** (1990), no. 5-6, 571–582, Computational group theory, Part 1. MR MR1075423 (91k:20022)

- [107] Gerhard O. Michler and Andrea Previtali, *Another existence and uniqueness proof for the Higman-Sims simple group*, Algebra Colloq. **12** (2005), no. 3, 369–398. MR MR2144992
- [108] Gerhard O. Michler and Øyvind Solberg, *Testing modules of groups of even order for simplicity*, J. Algebra **202** (1998), no. 1, 229–242. MR MR1614206 (99b:20008)
- [109] Gerhard O. Michler and Michael Weller, *A new computer construction of the irreducible 112-dimensional 2-modular representation of Janko’s group  $J_4$* , Comm. Algebra **29** (2001), no. 4, 1773–1806. MR MR1853125 (2002f:20020)
- [110] ———, *The character values of the irreducible constituents of a transitive permutation representation*, Arch. Math. (Basel) **78** (2002), no. 6, 417–429. MR MR1921730 (2003e:20008)
- [111] Vanessa Miemietz, *On representations of affine hecke algebras of type b*, Dissertation, Universität Stuttgart, 2005.
- [112] Torsten Minkwitz, *Extensions of irreducible representations*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 5, 391–399. MR MR1465078 (98d:20006)
- [113] Mohammad Reza R. Moghaddam, Ali Reza Salemkar, and Taghi Karimi, *Some inequalities for the order of the Schur multiplier of a pair of groups*, Comm. Algebra **36** (2008), no. 7, 2481–2486. MR MR2422499 (2009d:20016)
- [114] Alexander Moretó, *Complex group algebras of finite groups: Brauer’s problem 1*, Adv. Math. **208** (2007), no. 1, 236–248. MR MR2304316 (2008c:20011)
- [115] J. Neubüser, H. Pahlings, and W. Plesken, *CAS; design and use of a system for the handling of characters of finite groups*, Computational Group Theory (Durham, 1982), Academic Press, London, 1984, pp. 195–247. MR MR760658 (86i:20004)
- [116] Peter M. Neumann and Cheryl E. Praeger, *Cyclic matrices and the MEATAXE*, Groups and Computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 291–300. MR MR1829488 (2002d:20018)
- [117] E. A. O’Brien, *Towards effective algorithms for linear groups*, Finite Geometries, Groups, and Computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 163–190. MR MR2258009

- [118] Th. Ostermann, *Charaktertafeln von Sylownormalisatoren sporadischer einfacher Gruppen*, Vorlesungen aus dem Fachbereich Mathematik der Universität GH Essen [Lecture Notes in Mathematics at the University of Essen], vol. 14, Universität Essen Fachbereich Mathematik, Essen, 1986. MR MR872094 (88g:20002)
- [119] W. Plesken, *Finite unimodular groups of prime degree and circulants*, J. Algebra **97** (1985), no. 1, 286–312. MR MR812182 (87c:20020)
- [120] W. Plesken and D. Robertz, *Representations, commutative algebra, and Hurwitz groups*, J. Algebra **300** (2006), no. 1, 223–247. MR MR2228645
- [121] Wilhelm Plesken and Michael Pohst, *On maximal finite irreducible subgroups of  $GL(n, \mathbf{Z})$ . III. The nine-dimensional case*, Math. Comp. **34** (1980), no. 149, 245–258. MR MR551303 (81b:20012a)
- [122] ———, *On maximal finite irreducible subgroups of  $GL(n, \mathbf{Z})$ . IV. Remarks on even dimensions with applications to  $n = 8$* , Math. Comp. **34** (1980), no. 149, 259–275. MR MR551304 (81b:20012b)
- [123] ———, *On maximal finite irreducible subgroups of  $GL(n, \mathbf{Z})$ . V. The eight-dimensional case and a complete description of dimensions less than ten*, Math. Comp. **34** (1980), no. 149, 277–301, loose microfiche suppl. MR MR551305 (81b:20012c)
- [124] Andrea Previtali, *Unitriangular actions on quadratic forms and character degrees*, Linear Algebra Appl. **408** (2005), 120–150. MR MR2166858
- [125] ———, *Irreducible constituents of monomial representations*, J. Symbolic Comput. **41** (2006), no. 12, 1345–1359. MR MR2271329
- [126] M. Anwar Rao and Robert Sandling, *The characterisation of modular group algebras having unit groups of nilpotency class 3*, Canad. Math. Bull. **38** (1995), no. 1, 112–116. MR MR1319908 (96c:16044)
- [127] ———, *Vanishing orbit sums in group algebras of  $p$ -groups*, Groups '93 Galway/St. Andrews, Vol. 2, London Math. Soc. Lecture Note Ser., vol. 212, Cambridge Univ. Press, Cambridge, 1995, pp. 507–511. MR MR1337292 (96c:16034)
- [128] William F. Reynolds, *Noncommutators and the number of projective characters of a finite group*, The Arcata Conference on Representations of Finite Groups (Arcata,

- Calif., 1986), Proc. Sympos. Pure Math., vol. 47, Amer. Math. Soc., Providence, RI, 1987, pp. 71–74. MR MR933401 (89c:20027)
- [129] Daniel Robbins, *Broue’s abelian defect group conjecture for the Tits group*, 2008.
- [130] Robert Sandling, *The modular group algebra of a central-elementary-by-abelian  $p$ -group*, Arch. Math. (Basel) **52** (1989), no. 1, 22–27. MR MR980047 (90b:20007)
- [131] Travis Schedler, *Hochschild homology of preprojective algebras over the integers*, 2007.
- [132] Gerhard J. A. Schneider, *The vertices of the simple modules of  $M_{12}$  over a field of characteristic 2*, J. Algebra **83** (1983), no. 1, 189–200. MR MR710594 (84i:20013)
- [133] ———, *PSL(3, 4) in characteristic 3*, Comm. Algebra **15** (1987), no. 8, 1543–1547. MR MR884759 (88d:20020)
- [134] ———, *The structure of the projective indecomposable modules of the Suzuki group Sz(8) in characteristic 2*, Math. Comp. **60** (1993), no. 202, 779–786, S29–S32. MR MR1181331 (93h:20011)
- [135] Michael C. Slattery, *Character degrees of finite  $p$ -groups*, The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), Proc. Sympos. Pure Math., vol. 47, Amer. Math. Soc., Providence, RI, 1987, pp. 89–92. MR MR933404
- [136] ———, *Character degrees and derived length in  $p$ -groups*, Glasgow Math. J. **30** (1988), no. 2, 221–230. MR MR942995 (89g:20017)
- [137] Michael C. Slattery, *Character degrees of normally monomial maximal class 5-groups*, Contemporary Mathematics **524** (2010), 153–159.
- [138] Bernd Souvignier, *Decomposing homogeneous modules of finite groups in characteristic zero*, J. Algebra **322** (2009), no. 3, 948–956.
- [139] Britta Späth, *The McKay conjecture for exceptional groups and odd primes*, Math. Z. **Online first** (2008), 25.
- [140] Peter Symonds, *Cyclic group actions on polynomial rings*, Bull. Lond. Math. Soc. **39** (2007), no. 2, 181–188. MR MR2323446
- [141] Katsushi Waki, *Calculation of direct summands of FG-modules*, Sci. Rep. Hirosaki Univ. **44** (1997), no. 2, 193–200. MR MR1619001 (99c:16006)

- [142] Michael Weller, *Construction of large permutation representations for matrix groups II*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 463–488. MR MR1831941 (2002j:20031)
- [143] Mark Wildon, *Character values and decomposition matrices of symmetric groups*, J. Algebra **319** (2008), no. 8, 3382–3397. MR MR2408324 (2009c:20018)
- [144] ———, *Multiplicity-free representations of symmetric groups*, J. Pure Appl. Algebra **213** (2009), no. 7, 1464–1477. MR MR2497590
- [145] Pawel Wocjan, Martin Rötteler, Dominik Janzing, and Thomas Beth, *Universal simulation of Hamiltonians using a finite set of control operations*, Quantum Inf. Comput. **2** (2002), no. 2, 133–150. MR MR1910083 (2003e:81036)
- [146] Martin Wursthorn, *Isomorphisms of modular group algebras: an algorithm and its application to groups of order  $2^6$* , J. Symbolic Comput. **15** (1993), no. 2, 211–227. MR MR1218760 (94h:20008)

# Abstract Finite Groups

20Dxx

- [1] A. Adem, J. F. Carlson, D. B. Karagueuzian, and R. James Milgram, *The cohomology of the Sylow 2-subgroup of the Higman-Sims group*, J. Pure Appl. Algebra **164** (2001), no. 3, 275–305. MR MR1857743 (2002g:20089)
- [2] Faryad Ali and Jamshid Moori, *Fischer-Clifford matrices of the non-split group extension  $2^6 \cdot U_4(2)$* , Quaest. Math. **31** (2008), no. 1, 27–36. MR MR2404644
- [3] Habib Amiri, S. M. Jafarian Amiri, and I. M. Isaacs, *Sums of element orders in finite groups*, Comm. Algebra **37** (2009), no. 9, 2978–2980. MR MR2554185
- [4] Jianbei An, John J. Cannon, E. A. O'Brien, and W. R. Unger, *The Alperin weight conjecture and Dade's conjecture for the simple group  $\text{Fi}'_{24}$* , LMS J. Comput. Math. **11** (2008), 100–145. MR MR2410917
- [5] Michael Aschbacher and Marshall Hall, Jr., *Groups generated by a class of elements of order 3*, Finite groups '72 (Proc. Gainesville Conf., Univ. Florida, Gainesville, Fla., 1972), North-Holland Amsterdam, 1973, pp. 12–18. North-Holland Math. Studies, Vol. 7. MR MR0360794 (50 #13241)
- [6] Sarah Astill, *3-local identifications of some finite simple groups*, Ph.D. thesis, University of Birmingham, 2007.
- [7] Sarah Astill and Chris Parker, *A 3-local characterization of  $M_{12}$  and  $\text{SL}_3(3)$* , Arch. Math. (Basel) **92** (2009), no. 2, 99–110. MR MR2481505
- [8] Roberto M. Avanzi, Mathias Kratzer, and Gerhard O. Michler, *Janko's simple groups  $J_2$  and  $J_3$  are irreducible subgroups of  $\text{SL}_{85}(5)$  with equal centralizers of an involution*, Groups and Computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 21–37. MR MR1829469 (2002d:20016)
- [9] Nir Avni and Shelly Garion, *Connectivity of the product replacement graph of simple groups of bounded Lie rank*, J. Algebra **320** (2008), no. 2, 945–960. MR MR2422323
- [10] Henrik Bäårnhelm, *Recognising the Suzuki groups in their natural representations*, J. Algebra **300** (2006), no. 1, 171–198. MR MR2228642 (2007f:20031)

- [11] Robert F. Bailey and John N. Bray, *Decoding the Mathieu group  $M_{12}$* , Adv. Math. Commun. **1** (2007), no. 4, 477–487. MR MR2354049
- [12] Tatiana Bandman, Gert-Martin Greuel, Fritz Grunewald, Boris Kunyavskii, Gerhard Pfister, and Eugene Plotkin, *Two-variable identities for finite solvable groups*, C. R. Math. Acad. Sci. Paris **337** (2003), no. 9, 581–586. MR MR2017730 (2004i:20029)
- [13] ———, *Identities for finite solvable groups and equations in finite simple groups*, Compos. Math. **142** (2006), no. 3, 734–764. MR MR2231200 (2007d:20027)
- [14] Richard William Barraclough, *Some calculations related to the monster group*, Ph.D. thesis, University of Birmingham, September 2005, p. 129.
- [15] C. Bates, D. Bundy, S. Hart, and P. Rowley, *Commuting involution graphs for sporadic simple groups*, J. Algebra **316** (2007), no. 2, 849–868. MR MR2358617
- [16] Chris Bates and Peter Rowley, *Involutions in Conway’s largest simple group*, LMS J. Comput. Math. **7** (2004), 337–351 (electronic). MR MR2118178 (2005j:20017)
- [17] ———, *Normalizers of  $p$ -subgroups in finite groups*, Arch. Math. (Basel) **92** (2009), no. 1, 7–13. MR MR2471982
- [18] Chris Bates and Peter J. Rowley, *Centralizers of strongly real elements in finite groups*, 2003.
- [19] Barbara Baumeister and Alexander Stein, *Commuting graphs of odd prime order elements in simple groups*, 2009.
- [20] Sarah Marie Belcastro and Gary J. Sherman, *Counting centralizers in finite groups*, Math. Mag. **67** (1994), no. 5, 366–374. MR MR1307800 (95k:20029)
- [21] Thomas R. Berger and Marcel Herzog, *Criteria for nonperfectness*, Comm. Algebra **6** (1978), no. 9, 959–968. MR MR0491948 (58 #11119)
- [22] Hans Ulrich Besche and Bettina Eick, *The groups of order at most 1000 except 512 and 768*, J. Symbolic Comput. **27** (1999), no. 4, 405–413. MR MR1681347 (2000c:20002)
- [23] Hans Ulrich Besche, Bettina Eick, and E. A. O’Brien, *The groups of order at most 2000*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 1–4 (electronic). MR MR1826989

- [24] ———, *A millennium project: Constructing small groups*, *Internat. J. Algebra Comput.* **12** (2002), no. 5, 623–644. MR MR1935567 (2003h:20042)
- [25] Sean W. Bolt, John N. Bray, and Robert T. Curtis, *Symmetric presentation of the Janko group  $J_4$* , *J. Lond. Math. Soc. (2)* **76** (2007), no. 3, 683–701. MR MR2377119 (2008j:20040)
- [26] Nigel Boston, *Embedding 2-groups in groups generated by involutions*, *J. Algebra* **300** (2006), no. 1, 73–76. MR MR2228635 (2007e:20037)
- [27] Nigel Boston and Judy L. Walker, *2-groups with few conjugacy classes*, *Proc. Edinburgh Math. Soc. (2)* **43** (2000), no. 1, 211–217. MR MR1744712 (2000m:20045)
- [28] J. D. Bradley and R. T. Curtis, *Symmetric generation and existence of  $J_3 : 2$ , the automorphism group of the third Janko group*, *J. Algebra* **304** (2006), no. 1, 256–270. MR MR2256388 (2008e:20031)
- [29] ———, *Symmetric generation and existence of  $\text{McL} : 2$ , the automorphism group of the McLaughlin group*, *Comm. Algebra* **38** (2010), no. 2, 601–617. MR 2598901
- [30] L. Brailovsky, *On  $(3, m)$ -special elements in groups*, *Comm. Algebra* (1992), no. 11, 3301–3320. MR MR1186709 (94f:20043)
- [31] Rolf Brandl and Libero Verardi, *Finite simple groups with few conjugacy classes of subgroups*, *Japan. J. Math. (N.S.)* **18** (1992), no. 2, 347–359. MR MR1208191 (94d:20018)
- [32] J. N. Bray, R. T. Curtis, C. W. Parker, and C. B. Wiedorn, *Symmetric presentations for the Fischer groups. I. The classical groups  $\text{Sp}_6(2)$ ,  $\text{Sp}_8(2)$ , and  $3 \cdot \text{O}_7(3)$* , *J. Algebra* **265** (2003), no. 1, 171–199. MR MR1984905 (2004e:20021)
- [33] John Bray and Henrik Bäärnhielm, *Standard generators for the Suzuki groups*, 2008, pp. 1–13.
- [34] John N. Bray, Ibrahim A. I. Suleiman, Peter G. Walsh, and Robert A. Wilson, *Generating maximal subgroups of sporadic simple groups*, *Comm. Algebra* **29** (2001), no. 3, 1325–1337. MR MR1842416 (2002e:20032)
- [35] John N. Bray, John S. Wilson, and Robert A. Wilson, *A characterization of finite soluble groups by laws in two variables*, *Bull. London Math. Soc.* **37** (2005), no. 2, 179–186. MR MR2119017 (2005k:20035)



- [36] John N. Bray and Robert A. Wilson, *Explicit representations of maximal subgroups of the Monster*, J. Algebra **300** (2006), no. 2, 834–857. MR MR2228224 (2007c:20035)
- [37] ———, *On the orders of automorphism groups of finite groups. II*, J. Group Theory **9** (2006), no. 4, 537–545. MR MR2243245 (2007d:20044)
- [38] F. Buekenhout and M. Hermand, *On flag-transitive geometries and groups*, Travaux de Mathématiques de l'Université Libre de Bruxelles **1** (1991), 45–78.
- [39] Francis Buekenhout, *The geometry of the finite simple groups*, Buildings and the Geometry of Diagrams (Como, 1984), Lecture Notes in Math., vol. 1181, Springer, Berlin, 1986, pp. 1–78. MR MR843389 (87h:20032)
- [40] ———, *Finite groups and geometries: A view on the present state and on the future*, Groups of Lie Type and their Geometries (Como, 1993), London Math. Soc. Lecture Note Ser., vol. 207, Cambridge Univ. Press, Cambridge, 1995, pp. 35–42. MR MR1320513 (96a:51006)
- [41] Francis Buekenhout and Dimitri Leemans, *On a geometry of Ivanov and Shpectorov for the O'Nan sporadic simple group*, J. Combin. Theory Ser. A **85** (1999), no. 2, 148–164. MR MR1673924 (2000a:51014)
- [42] Francis Buekenhout and Sarah Rees, *The subgroup structure of the Mathieu group  $M_{12}$* , Math. Comp. **50** (1988), no. 182, 595–605. MR MR929556 (88m:20024)
- [43] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev, *Base sizes for simple groups and a conjecture of Cameron*, Proc. Lond. Math. Soc. (3) **98** (2009), no. 1, 116–162. MR MR2472163 (2009m:20001)
- [44] G. Butler, *The maximal subgroups of the Chevalley group  $G_2(4)$* , Groups—St. Andrews 1981 (St. Andrews, 1981), London Math. Soc. Lecture Note Ser., vol. 71, Cambridge Univ. Press, Cambridge, 1982, pp. 186–200. MR MR679160 (84e:20014)
- [45] Gregory Butler, *The maximal subgroups of the sporadic simple group of Held*, J. Algebra **69** (1981), no. 1, 67–81. MR MR613857 (82e:20022)
- [46] Colin Campbell, George Havas, Stephen Linton, and Edmund Robertson, *Symmetric presentations and orthogonal groups*, The Atlas of Finite Groups: Ten Years On (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, Cambridge, 1998, pp. 1–10. MR MR1647409 (99m:20112)

- [47] Colin M. Campbell, George Havas, Colin Ramsay, and Edmund F. Robertson, *Nice efficient presentations for all small simple groups and their covers*, LMS J. Comput. Math. **7** (2004), 266–283 (electronic). MR MR2118175 (2006g:20046)
- [48] ———, *On the efficiency of the simple groups of order less than a million and their covers*, Experiment. Math. **16** (2007), no. 3, 347–358. MR MR2367323 (2009a:20051)
- [49] John J. Cannon, John McKay, and Kiang Chuen Young, *The nonabelian simple groups  $G$ ,  $|G| < 10^5$  — presentations*, Comm. Algebra **7** (1979), no. 13, 1397–1406. MR MR539356 (80e:20023)
- [50] David P. Cargo, Warwick de Launey, Martin W. Liebeck, and Richard M. Stafford, *Short two-variable identities for finite groups*, J. Group Theory **11** (2008), no. 5, 675–690. MR MR2446149 (2009g:20047)
- [51] Jon F. Carlson, *Maximal elementary abelian subgroups of rank 2*, J. Group Theory **10** (2007), no. 1, 5–13. MR MR2288455
- [52] ———, *The poset of elementary abelian  $p$ -subgroups having rank at least 2*, J. Group Theory (To appear).
- [53] Marston Conder, *Random walks in large finite groups*, Australas. J. Combin. **4** (1991), 49–57, Combinatorial mathematics and combinatorial computing (Palmerston North, 1990). MR MR1129268 (92h:20030)
- [54] ———, *The symmetric genus of the Mathieu groups*, Bull. London Math. Soc. **23** (1991), no. 5, 445–453. MR MR1141014 (92k:20023)
- [55] Marston Conder, George Havas, and Colin Ramsay, *Efficient presentations for the Mathieu simple group  $M_{22}$  and its cover*, Finite geometries, groups, and computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 33–41. MR MR2257999 (2007e:20027)
- [56] Marston Conder and I. M. Isaacs, *Derived subgroups of products of an abelian and a cyclic subgroup*, J. London Math. Soc. (2) **69** (2004), no. 2, 333–348. MR MR2040608 (2005e:20030)
- [57] Marston Conder, R. A. Wilson, and A. J. Woldar, *The symmetric genus of sporadic groups*, Proc. Amer. Math. Soc. **116** (1992), no. 3, 653–663. MR MR1126192 (93a:20027)

- [58] ———, *The symmetric genus of sporadic groups: Announced results*, Coding Theory, Design Theory, Group Theory (Burlington, VT, 1990), Wiley-Intersci. Publ., Wiley, New York, 1993, pp. 163–169. MR MR1227128 (94f:20033)
- [59] S. B. Conlon, *p-groups with an abelian maximal subgroup and cyclic center*, J. Austral. Math. Soc. Ser. A **22** (1976), no. 2, 221–233. MR MR0427458 (55 #490)
- [60] G. D. Cooperman, W. Lempken, G. O. Michler, and M. Weller, *A new existence proof of Janko's simple group  $J_4$* , Computational methods for representations of groups and algebras (Essen, 1997), Progr. Math., vol. 173, Birkhäuser, Basel, 1999, pp. 161–175. MR MR1714608 (2000g:20028)
- [61] John Cossey and Trevor Hawkes, *On the largest conjugacy class size in a finite group*, Rend. Sem. Mat. Univ. Padova **103** (2000), 171–179. MR MR1789537 (2001i:20063)
- [62] John Cossey and Stewart E. Stonehewer, *The embedding of a cyclic permutable subgroup in a finite group*, Illinois J. Math. **47** (2003), no. 1-2, 89–111, Special issue in honor of Reinhold Baer (1902–1979). MR MR2031309 (2004j:20042)
- [63] R. T. Curtis, *Natural constructions of the Mathieu groups*, Math. Proc. Cambridge Philos. Soc. **106** (1989), no. 3, 423–429. MR MR1010366 (90h:20020)
- [64] ———, *Symmetric generation of the Higman-Sims group*, J. Algebra **171** (1995), no. 2, 567–586. MR MR1315913 (96b:20018)
- [65] ———, *Symmetric generation and existence of the Janko group  $J_1$* , J. Group Theory **2** (1999), no. 4, 355–366. MR MR1718738 (2001d:20016)
- [66] R. T. Curtis and B. T. Fairbairn, *Symmetric representation of the elements of the Conway group  $\cdot 0$* , J. Symbolic Comput. **44** (2009), no. 8, 1044–1067. MR MR2523767
- [67] R. T. Curtis and Z. Hasan, *Symmetric representation of the elements of the Janko group  $J_1$* , J. Symbolic Comput. **22** (1996), no. 2, 201–214. MR MR1422146 (97m:20024)
- [68] Robert T. Curtis, *Symmetric generation of groups*, Encyclopedia of Mathematics and its Applications, vol. 111, Cambridge University Press, Cambridge, 2007, With applications to many of the sporadic finite simple groups. MR MR2375232

- [69] M. R. Darafsheh, A. R. Ashrafi, and G. A. Moghani, *(p, q, r)*-generations of the Conway group  $\text{Co}_1$  for odd  $p$ , *Kumamoto J. Math.* **14** (2001), 1–20. MR MR1835386 (2002d:20020)
- [70] Alice Devillers, Michael Giudici, Cai Heng Li, Geoffrey Pearce, and Cheryl E. Praeger, *On imprimitive rank 3 permutation groups*, 2010.
- [71] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *Locally  $s$ -distance transitive graphs*, 2010.
- [72] Bettina Eick, M. F. Newman, and E. A. O’Brien, *The class-breadth conjecture revisited*, *J. Algebra* **300** (2006), no. 1, 384–393. MR MR2228655 (2007c:20044)
- [73] Bettina Eick and E. A. O’Brien, *Enumerating  $p$ -groups*, *J. Austral. Math. Soc. Ser. A* **67** (1999), no. 2, 191–205, Group theory. MR MR1717413 (2000h:20033)
- [74] Ben Elias, Lior Silberman, and Ramin Takloo-Bighash, *Minimal permutation representations of nilpotent groups*, *Experiment. Math.* **19** (2010), no. 1, 121–128.
- [75] Anthony B. Evans, *The admissibility of sporadic simple groups*, *Journal of Algebra* **321** (2009), no. 1, 105 – 116.
- [76] Susan Evans-Riley, *On the derived length of finite, graded Lie rings with prime-power order and groups with prime-power order.*, *Bull. Austral. Math. Soc.* **64** (2001), no. 1, 171–172.
- [77] Susan Evans-Riley, M. F. Newman, and Csaba Schneider, *On the soluble length of groups with prime-power order*, *Bull. Austral. Math. Soc.* **59** (1999), no. 2, 343–346. MR MR1680838 (2000b:20021)
- [78] Ben Fairbairn, *Improved upper bounds on the spreads of some large sporadic groups*, 2009.
- [79] ———, *Recent progress in the symmetric generation of groups*, 2010.
- [80] Reza Rezaeian Farashahi, Ruud Pellikaan, and Andrey Sidorenko, *Extractors for binary elliptic curves*, *Des. Codes Cryptogr.* **49** (2008), no. 1-3, 171–186. MR MR2438449
- [81] J. Fischer and J. McKay, *The nonabelian simple groups  $G$ ,  $|G| < 10^6$ —maximal subgroups*, *Math. Comp.* **32** (1978), no. 144, 1293–1302. MR MR0498831 (58 #16867)

- [82] Tuval Foguel, *Groups, transversals, and loops*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 261–269, Loops’99 (Prague). MR MR1780870 (2001h:20099)
- [83] A. Fukshansky and G. Stroth, *Semiclassical parabolic systems related to  $M_{24}$* , Geom. Dedicata **70** (1998), no. 3, 305–329. MR MR1624018 (99d:20023)
- [84] Shelly Garion and Aner Shalev, *Commutator maps, measure preservation, and  $T$ -systems*, Trans. Amer. Math. Soc. **361** (2009), no. 9, 4631–4651. MR MR2506422
- [85] Volker Gebhardt, *Two short presentations for Lyons’ sporadic simple group*, Experiment. Math. **9** (2000), no. 3, 333–338. MR MR1795305 (2001j:20021)
- [86] Michael Giudici, *Factorisations of sporadic simple groups*, J. Algebra **304** (2006), no. 1, 311–323. MR MR2256393
- [87] Holger W. Gollan, *A new existence proof for  $Ly$ , the sporadic simple group of  $R$ . Lyons*, J. Symbolic Comput. **31** (2001), no. 1-2, 203–209, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806216 (2001j:20022)
- [88] María Isabel González Vasco, Martin Rötteler, and Rainer Steinwandt, *On minimal length factorizations of finite groups*, Experiment. Math. **12** (2003), no. 1, 1–12. MR MR2002670 (2004h:20035)
- [89] Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii, and Eugene Plotkin, *On the number of conjugates defining the solvable radical of a finite group*, C. R. Math. Acad. Sci. Paris **343** (2006), no. 6, 387–392. MR MR2259878 (2007f:20032)
- [90] Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii, and Eugene Plotkin, *A commutator description of the solvable radical of a finite group*, Groups Geom. Dyn. **2** (2008), no. 1, 85–120. MR MR2367209 (2008j:20057)
- [91] ———, *A description of Baer-Suzuki type of the solvable radical of a finite group*, J. Pure Appl. Algebra **213** (2009), no. 2, 250–258. MR MR2467402 (2009i:20045)
- [92] Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii, and Eugene Plotkin, *From Thompson to Baer-Suzuki: A sharp characterization of the solvable radical*, J. Algebra **323** (2010), no. 10, 2888–2904.
- [93] Simon Guest, *A solvable version of the Baer–Suzuki theorem*, Trans. Amer. Math. Soc. **362** (2010), 5909–5946. MR MR2661502

- [94] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky, *Presentations of finite simple groups: A quantitative approach*, J. Amer. Math. Soc. **21** (2008), no. 3, 711–774. MR MR2393425
- [95] George Havas and Charles C. Sims, *A presentation for the Lyons simple group*, Computational methods for representations of groups and algebras (Essen, 1997), Progr. Math., vol. 173, Birkhäuser, Basel, 1999, pp. 241–249. MR MR1714614 (2000g:20030)
- [96] T. Hawkes, I. M. Isaacs, and M. Özaydin, *On the Möbius function of a finite group*, Rocky Mountain J. Math. **19** (1989), no. 4, 1003–1034. MR MR1039540 (90k:20046)
- [97] P. E. Holmes, *On minimal factorisations of sporadic groups*, Experiment. Math. **13** (2004), no. 4, 435–440. MR MR2118268 (2005k:20032)
- [98] ———, *A classification of subgroups of the Monster isomorphic to  $S_4$  and an application*, J. Algebra **319** (2008), no. 8, 3089–3099. MR MR2408306 (2009b:20023)
- [99] P. E. Holmes and R. A. Wilson, *A new maximal subgroup of the Monster*, J. Algebra **251** (2002), no. 1, 435–447. MR MR1900293 (2003d:20022)
- [100] Petra E. Holmes and Robert A. Wilson, *A new computer construction of the Monster using 2-local subgroups*, J. London Math. Soc. (2) **67** (2003), no. 2, 349–364. MR MR1956140 (2003k:20017)
- [101] Derek F. Holt and Colva M. Roney-Dougal, *Constructing maximal subgroups of classical groups*, LMS J. Comput. Math. **8** (2005), 46–79 (electronic). MR MR2123130 (2005k:20027)
- [102] A. Jaikin-Zapirain, M. F. Newman, and E. A. O’Brien, *On  $p$ -groups having the minimal number of conjugacy classes of maximal size*, Israel J. Math. **172** (2009), 119–123. MR MR2534242
- [103] Rodney James, M. F. Newman, and E. A. O’Brien, *The groups of order 128*, J. Algebra **129** (1990), no. 1, 136–158. MR MR1037398 (90j:20050)
- [104] David Joyner, Richard Kreminski, and Joann Turisco, *Applied abstract algebra*, Johns Hopkins University Press, Baltimore, MD, 2004. MR MR2378252
- [105] W. F. Ke and K. S. Wang, *On the Frobenius groups with kernel of order 64*, Contributions to general algebra, 7 (Vienna, 1990), Hölder-Pichler-Tempsky, Vienna, 1991, pp. 221–233. MR MR1143086 (93c:20054)

- [106] Hyun Kyu Kim, *Representation theoretic existence proof for Fischer group  $Fi_{23}$* , Honours thesis, Cornell University, 2009.
- [107] Hyun Kyu Kim and Gerhard O. Michler, *Construction of  $Co_1$  from an irreducible subgroup  $M_{24}$  of  $GL_{11}(2)$* , 2009.
- [108] Joachim König, *Solvability of generalized monomial groups*, 2009.
- [109] M. Kratzer, G. O. Michler, and M. Weller, *Harada group uniquely determined by centralizer of a 2-central involution*, Proceedings of the First Sino-German Workshop on Representation Theory and Finite Simple Groups (Beijing, 2002), vol. 10, 2003, pp. 303–372. MR MR2014018 (2004h:20020)
- [110] Mathias Kratzer, *Uniform and natural existence proofs for Janko’s sporadic groups  $J_2$  and  $J_3$* , Arch. Math. (Basel) **79** (2002), no. 1, 5–18. MR MR1923032 (2003g:20027)
- [111] Mathias Kratzer, Wolfgang Lempken, Gerhard O. Michler, and Katsushi Waki, *Another existence and uniqueness proof for McLaughlin’s simple group*, J. Group Theory **6** (2003), no. 4, 443–459. MR MR2007740 (2004i:20027)
- [112] J. L. Leavitt, G. J. Sherman, and M. E. Walker, *Rewriteability in finite groups*, Amer. Math. Monthly **99** (1992), no. 5, 446–452. MR MR1163633 (93c:20047)
- [113] Dimitri Leemans, *The rank 2 geometries of the simple Suzuki groups  $Sz(q)$* , Beiträge Algebra Geom. **39** (1998), no. 1, 97–120. MR MR1614433 (99b:20030)
- [114] ———, *On a rank four geometry for the Hall-Janko sporadic group*, J. Combin. Theory Ser. A **101** (2003), no. 1, 160–167. MR MR1953287 (2004a:20023)
- [115] Dimitri Leemans, *On computing the subgroup lattice of  $O’N$* , 2008, p. 23.
- [116] Dimitri Leemans, *Locally  $s$ -arc-transitive graphs related to sporadic simple groups*, J. Algebra **322** (2009), no. 3, 882–892. MR MR2531226
- [117] Wolfgang Lempken, *On the existence and uniqueness of the sporadic simple groups  $J_2$  and  $J_3$  of  $Z$ . Janko*, J. Group Theory **4** (2001), no. 2, 223–232. MR MR1812328 (2002b:20021)
- [118] ———, *2-local amalgams for the simple groups  $GL(5, 2)$ ,  $M_{24}$  and  $He$ . II*, Proceedings of the First Sino-German Workshop on Representation Theory and Finite Simple Groups (Beijing, 2002), vol. 10, 2003, pp. 373–380. MR MR2014019 (2004h:20021)

- [119] ———, *2-local amalgams for the simple groups  $GL(5, 2)$ ,  $M_{24}$  and He*, Illinois J. Math. **47** (2003), no. 1-2, 361–393, Special issue in honor of Reinhold Baer (1902–1979). MR MR2031329 (2004m:20035)
- [120] ———, *On 2-local amalgams proving existence and uniqueness of  $McL$  and  $3.McL$* , IEM, Essen. 2002.
- [121] Mark L. Lewis, *Brauer pairs of Camina  $p$ -groups of nilpotence class 2*, Arch. Math. (Basel) **92** (2009), no. 2, 95–98. MR MR2481504
- [122] Martin W. Liebeck, Aner Shalev, Pham Huu Tiep, and E.A. O’Brien, *The Ore conjecture*, 2008.
- [123] F. Lübeck, K. Magaard, and E. A. O’Brien, *Constructive recognition of  $SL_3(q)$* , J. Algebra **316** (2007), no. 2, 619–633. MR MR2356848
- [124] Arturo Magidin, *Capability of nilpotent products of cyclic groups*, J. Group Theory **8** (2005), no. 4, 431–452. MR MR2152690 (2006c:20073)
- [125] John McKay and Kiang Chuen Young, *The nonabelian simple groups  $G$ ,  $|G| < 10^6$  — minimal generating pairs*, Math. Comp. **33** (1979), no. 146, 812–814. MR MR521296 (80d:20018)
- [126] Gerhard O. Michler, *On the uniqueness of the finite simple groups with a given centralizer of a 2-central involution*, Illinois J. Math. **47** (2003), no. 1-2, 419–444, Special issue in honor of Reinhold Baer (1902–1979). MR MR2031331 (2005b:20025)
- [127] Gerhard O. Michler, *Theory of finite simple groups*, first ed., New Mathematical Monographs, vol. 8, Cambridge University Press, Cambridge, 2006.
- [128] Gerhard O. Michler and Andrea Previtali, *Another existence and uniqueness proof for the Higman-Sims simple group*, Algebra Colloq. **12** (2005), no. 3, 369–398. MR MR2144992
- [129] ———, *O’Nan group uniquely determined by the centralizer of a 2-central involution*, J. Algebra Appl. **6** (2007), no. 1, 135–171. MR MR2302699 (2009a:20029)
- [130] Gerhard O. Michler and Lizhong Wang, *Another existence and uniqueness proof of the Tits group*, Algebra Colloq. **15** (2008), no. 2, 241–278. MR MR2400182



- [131] Gerhard O. Michler, Michael Weller, and Katsushi Waki, *Natural existence proof for Lyons simple group*, J. Algebra Appl. **2** (2003), no. 3, 277–315. MR MR1997749 (2004i:20028)
- [132] Jamshid Moori, *Subgroups of 3-transposition groups generated by four 3-transpositions*, Quaestiones Math. **17** (1994), no. 1, 83–94. MR MR1276010 (95d:20032)
- [133] M. F. Newman and E. A. O’Brien, *Classifying 2-groups by coclass*, Trans. Amer. Math. Soc. **351** (1999), no. 1, 131–169. MR MR1458332 (99c:20020)
- [134] M. F. Newman, E. A. O’Brien, and M. R. Vaughan-Lee, *Groups and nilpotent Lie rings whose order is the sixth power of a prime*, J. Algebra **278** (2004), no. 1, 383–401. MR MR2068084 (2005c:20034)
- [135] Jeanne Nielsen, *Rewritable sequencing of groups*, Ars Combin. **36** (1993), 207–214. MR MR1246914 (94m:20058)
- [136] Simon Norton, *Computing in the Monster*, J. Symbolic Comput. **31** (2001), no. 1-2, 193–201, Computational algebra and number theory (Milwaukee, WI, 1996 ). MR MR1806215 (2001k:20029)
- [137] E. A. O’Brien, *The groups of order 256*, J. Algebra **143** (1991), no. 1, 219–235. MR MR1128656 (93e:20029)
- [138] E. A. O’Brien and M. R. Vaughan-Lee, *The groups with order  $p^7$  for odd prime  $p$* , J. Algebra **292** (2005), no. 1, 243–258. MR MR2166803
- [139] E. A. O’Brien and Michael Vaughan-Lee, *The 2-generator restricted Burnside group of exponent 7*, Internat. J. Algebra Comput. **12** (2002), no. 4, 575–592. MR MR1919689 (2003i:20032)
- [140] Elizabeth A. Ormerod, *On the Wielandt length of metabelian  $p$ -groups*, Arch. Math. (Basel) **57** (1991), no. 3, 212–215. MR MR1119892 (92m:20016)
- [141] Christopher Parker, *Generators and relations for the Lyons sporadic simple group*, Arch. Math. (Basel) **78** (2002), no. 2, 97–103. MR MR1888009 (2002m:20030)
- [142] Christopher Parker and Peter Rowley, *Classical groups in dimension 3 as completions of the Goldschmidt  $G_3$ -amalgam*, J. London Math. Soc. (2) **62** (2000), no. 3, 802–812. MR MR1794286 (2001j:20019)

- [143] ———, *Sporadic simple groups which are completions of the Goldschmidt  $G_3$ -amalgam*, J. Algebra **235** (2001), no. 1, 131–153. MR MR1807659 (2001k:20030)
- [144] ———, *Local characteristic  $p$  completions of weak BN-pairs*, Proc. London Math. Soc. (3) **93** (2006), no. 2, 325–394. MR MR2251156
- [145] ———, *A 3-local identification of the alternating group of degree 8, the McLaughlin simple group and their automorphism groups*, J. Algebra **319** (2008), no. 4, 1752–1775. MR MR2383065 (2009b:20024)
- [146] M. A. Pellegrini and M. C. Tamburini, *Hurwitz generation of the universal covering of  $Alt(n)$* , J. Group Theory **13** (2010), no. 5, 649–657.
- [147] Colin Reid, *A problem in the Kourovka notebook concerning the number of conjugacy classes of a finite group*, 2008.
- [148] Evija Ribnere, *Sequences of words characterizing finite solvable groups*, Monatsh. Math. **157** (2009), no. 4, 387–401. MR MR2520689
- [149] José L. Rodríguez, Jérôme Scherer, and Antonio Viruel, *Non-simple localizations of finite simple groups*, J. Algebra **305** (2006), no. 2, 765–774. MR MR2266851
- [150] Mohamed Sayed, *Combinatorial method in the coset enumeration of symmetrically generated groups. II. Monomial modular representations*, Int. J. Algebra **1** (2007), no. 9-12, 505–518. MR MR2380980 (2008k:20067)
- [151] ———, *Combinatorial method in the coset enumeration of symmetrically generated groups*, Int. J. Comput. Math. **85** (2008), no. 7, 993–1001. MR MR2428981 (2009f:20001)
- [152] Csaba Schneider, *Some results on the Derived Series of Finite  $p$ -groups*, Ph D thesis, Australian National University, 1999.
- [153] Csaba Schneider, *Groups of prime-power order with a small second derived quotient*, J. Algebra **266** (2003), no. 2, 539–551. MR MR1995127 (2004e:20030)
- [154] ———, *Small derived quotients in finite  $p$ -groups*, Publ. Math. Debrecen **69** (2006), no. 3, 373–378. MR MR2273990
- [155] U. Schoenwaelder, *Finite groups with a Sylow 2-subgroup of type  $M_{24}$ . I, II*, J. Algebra **28** (1974), 20–45; *ibid.* **28** (1974), 46–56. MR MR0369511 (51 #5744)

- [156] Gary J. Sherman, Thomas J. Tucker, and Mark E. Walker, *How Hamiltonian can a finite group be?*, Arch. Math. (Basel) **57** (1991), no. 1, 1–5. MR MR1111106 (92f:20026)
- [157] Michael C. Slattery, *Generation of groups of square-free order*, J. Symbolic Comput. **42** (2007), no. 6, 668–677. MR MR2325920
- [158] Leonard H. Soicher, *A new uniqueness proof for the Held group*, Bull. London Math. Soc. **23** (1991), no. 3, 235–238. MR MR1123331 (92k:20025)
- [159] R. Staszewski, H. Völklein, and G. Wiesend, *Counting generating systems of a finite group from given conjugacy classes*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 256–263. MR MR2182044 (2006f:20002)
- [160] Mark Stather, *Constructive Sylow theorems for the classical groups*, J. Algebra **316** (2007), no. 2, 536–559. MR MR2356843
- [161] G. Stroth and R. Weiss, *A new construction of the group Ru*, Quart. J. Math. Oxford Ser. (2) **41** (1990), no. 162, 237–243. MR MR1053664 (91m:20025)
- [162] Gernot Stroth and Richard Weiss, *Modified Steinberg relations for the group  $J_4$* , Geom. Dedicata **25** (1988), no. 1-3, 513–525, Geometries and groups (Noordwijkerhout, 1986). MR MR925850 (89c:20032)
- [163] Ibrahim A. I. Suleiman and Robert A. Wilson, *Standard generators for  $J_3$* , Experiment. Math. **4** (1995), no. 1, 11–18. MR MR1359414 (96j:20024)
- [164] Fritz Grunewald Tatiana Bandman, Shelly Garion, *On the surjectivity of engel words on  $psl(2,q)$* , 2010, pp. 1–22.
- [165] John van Bon, Arjeh M. Cohen, and Hans Cuypers, *Graphs related to Held’s simple group*, J. Algebra **123** (1989), no. 1, 6–26. MR MR1000473 (90h:20019)
- [166] John van Bon and Richard Weiss, *A characterization of the groups  $Fi_{22}$ ,  $Fi_{23}$  and  $Fi_{24}$* , Forum Math. **4** (1992), no. 4, 425–432. MR MR1166264 (93d:20035)
- [167] Richard Weiss, *A geometric characterization of the groups  $M_{12}$ , He and Ru*, J. Math. Soc. Japan **43** (1991), no. 4, 795–814. MR MR1126150 (92k:20076)
- [168] ———, *A geometric characterization of the groups McL and  $Co_3$* , J. London Math. Soc. (2) **44** (1991), no. 2, 261–269. MR MR1136439 (93g:20035)

- [169] Michael Weller, Gerhard O. Michler, and Andrea Previtali, *Thompson's sporadic group uniquely determined by the centralizer of a 2-central involution*, J. Algebra **298** (2006), no. 2, 371–459. MR MR2217621 (2006m:20022)
- [170] Stewart Wilcox, *Reduction of the Hall-Paige conjecture to sporadic simple groups*, J. Algebra **321** (2009), no. 5, 1407–1428. MR MR2494397
- [171] J. B. Wilson, *Finding central decompositions of  $p$ -groups*, J. Group Theory **12** (2009), 813–830.
- [172] Robert A. Wilson, *New computations in the monster*, 2006, p. 11.
- [173] Şükrü Yalçinkaya, *Black box groups*, Turk. J. Math. **31** (2007), no. Suppl, 171–210.
- [174] Ivan Yudin, *Presentation for parabolic subgroups of  $GL_n(F_2)$* , 2010.

# Structure and Classification

20Exx

- [1] Barbara Baumeister and Alexander Stein, *Commuting graphs of odd prime order elements in simple groups*, 2009.
- [2] Gilbert Baumslag, Sean Cleary, and George Havas, *Experimenting with infinite groups. I*, *Experiment. Math.* **13** (2004), no. 4, 495–502. MR MR2118274 (2005i:20044)
- [3] Russell D. Blyth and Derek J. S. Robinson, *Insoluble groups with the rewriting property  $P_8$* , *J. Pure Appl. Algebra* **72** (1991), no. 3, 251–263. MR MR1120692 (93b:20055)
- [4] Alexandre V. Borovik, Evgenii I. Khukhro, and Alexei G. Myasnikov, *The Andrews-Curtis conjecture and black box groups*, *Internat. J. Algebra Comput.* **13** (2003), no. 4, 415–436. MR MR2022117 (2004k:20050)
- [5] Nigel Boston and Jordan S. Ellenberg, *Pro- $p$  groups and towers of rational homology spheres*, 2006, pp. 331–334 (electronic). MR MR2224459 (2007f:20052)
- [6] John Cannon and Derek F. Holt, *Computing maximal subgroups of finite groups*, *J. Symbolic Comput.* **37** (2004), no. 5, 589–609. MR MR2094616 (2005i:20047)
- [7] Lisa Carbone, Leigh Cobbs, and Scott H. Murray, *Fundamental domains for congruence subgroups of  $SL_2$  in positive characteristic*, 2009.
- [8] ———, *Fundamental domains for congruence subgroups of  $SL_2$  in positive characteristic*, 2011, pp. 431–439.
- [9] Donald I. Cartwright, *Groups acting simply transitively on the vertices of a building of type  $A_n$* , *Groups of Lie Type and Their Geometries (Como, 1993)*, *London Math. Soc. Lecture Note Ser.*, vol. 207, Cambridge Univ. Press, Cambridge, 1995, pp. 43–76. MR MR1320514 (96a:20039)
- [10] Donald I. Cartwright, Anna Maria Mantero, Tim Steger, and Anna Zappa, *Groups acting simply transitively on the vertices of a building of type  $A_2$ . I*, *Geom. Dedicata* **47** (1993), no. 2, 143–166. MR MR1232965 (95b:20053)
- [11] ———, *Groups acting simply transitively on the vertices of a building of type  $A_2$ . II. The cases  $q = 2$  and  $q = 3$* , *Geom. Dedicata* **47** (1993), no. 2, 167–223. MR MR1232966 (95b:20054)

- [12] Marston Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370. MR MR1041434 (91d:20032)
- [13] ———, *Group actions on the cubic tree*, J. Algebraic Combin. **1** (1992), no. 3, 209–218. MR MR1194075 (94b:20034)
- [14] Vincent Delwiche, *Recherche de notations structurales pour les groupes d'ordre inférieur ou égal à 100 à l'aide de cayley*, Dissertation, Université Libre De Bruxelles, 1990.
- [15] Jason S. Kimberley and Guyan Robertson, *Groups acting on products of trees, tiling systems and analytic K-theory*, New York J. Math. **8** (2002), 111–131 (electronic). MR MR1923572 (2003j:20042)
- [16] M. F. Newman, *On coclass and trivial Schur multiplier*, J. Algebra **322** (2009), no. 3, 910–913. MR MR2531229 (2010d:20024)
- [17] M. F. Newman and E. A. O'Brien, *Application of computers to questions like those of Burnside. II*, Internat. J. Algebra Comput. **6** (1996), no. 5, 593–605. MR MR1419133 (97k:20002)
- [18] Joseph J. Rotman, *An Introduction to the Theory of Groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995. MR MR1307623 (95m:20001)
- [19] G. Stroth, *Nonspherical spheres*, Groups, combinatorics & geometry (Durham, 1990), London Math. Soc. Lecture Note Ser., vol. 165, Cambridge Univ. Press, Cambridge, 1992, pp. 151–158. MR MR1200258 (93m:20036)

# Special Aspects of Finite or Infinite Groups

20Fxx

- [1] Roger C. Alperin, *Platonic triangles of groups*, Experiment. Math. **7** (1998), no. 3, 191–219. MR MR1676687 (2000e:20069)
- [2] Daniel Appel and Evija Ribnere, *On the index of congruence subgroups of  $\text{Aut}(F_n)$* , J. Algebra **321** (2009), no. 10, 2875–2889. MR MR2512632
- [3] Björn Assmann and Stephen Linton, *Using the Malcev correspondence for collection in polycyclic groups*, J. Algebra **316** (2007), no. 2, 828–848. MR MR2358616
- [4] Huseyin Aydin and Geoff C. Smith, *Finite  $p$ -quotients of some cyclically presented groups*, J. London Math. Soc. (2) **49** (1994), no. 1, 83–92. MR MR1253013 (94k:20059)
- [5] Tathagata Basak, *On Coxeter diagrams of complex reflection groups*, 2008.
- [6] C. Bates, D. Bundy, Sarah B. Perkins, and P. Rowley, *Commuting involution graphs for finite Coxeter groups*, J. Group Theory **6** (2003), no. 4, 461–476. MR MR2007741 (2004j:20082)
- [7] Joan S. Birman, Volker Gebhardt, and Juan González-Meneses, *Conjugacy in Garside groups. III. Periodic braids*, J. Algebra **316** (2007), no. 2, 746–776. MR MR2358613
- [8] Russell D. Blyth, *Rewriting products of group elements I*, J. Algebra **116** (1988), no. 2, 506–521. MR MR953167 (90b:20033)
- [9] ———, *Rewriting products of group elements II*, J. Algebra **119** (1988), no. 1, 246–259. MR MR971358 (90b:20034)
- [10] Russell D. Blyth and Robert Fitzgerald Morse, *Computing the nonabelian tensor squares of polycyclic groups*, J. Algebra **321** (2009), no. 8, 2139–2148. MR MR2501513
- [11] Russell D. Blyth and Derek J. S. Robinson, *Recent progress on rewritability in groups*, Group theory (Singapore, 1987), de Gruyter, Berlin, 1989, pp. 77–85. MR MR981835 (90b:20035)

- [12] ———, *Solution of the solubility problem for rewritable groups*, J. London Math. Soc. (2) **41** (1990), no. 3, 438–444. MR MR1072050 (91j:20102)
- [13] John N. Bray, *An improved method for generating the centralizer of an involution*, Arch. Math. (Basel) **74** (2000), no. 4, 241–245. MR MR1742633 (2001c:20063)
- [14] John N. Bray and Robert T. Curtis, *A systematic approach to symmetric presentations II: Generators of order 3*, Math. Proc. Cambridge Philos. Soc. **128** (2000), no. 1, 1–20. MR MR1724425 (2000k:20032)
- [15] Ronald Brown, Neil Ghani, Anne Heyworth, and Christopher D. Wensley, *String rewriting for double coset systems*, J. Symbolic Comput. **41** (2006), no. 5, 573–590. MR MR2209165 (2006m:20044)
- [16] John Burns and Graham Ellis, *On the nilpotent multipliers of a group*, Math. Z. **226** (1997), no. 3, 405–428. MR MR1483540 (98h:20050)
- [17] Bill Casselman, *Computation in Coxeter groups. II. Constructing minimal roots*, Represent. Theory **12** (2008), 260–293. MR MR2439007
- [18] Alberto Cavicchioli, E. A. O’Brien, and Fulvia Spaggiari, *On some questions about a family of cyclically presented groups*, J. Algebra **320** (2008), no. 11, 4063–4072. MR MR2464807
- [19] Arjeh M. Cohen and Luis Paris, *On a theorem of Artin*, J. Group Theory **6** (2003), no. 4, 421–441. MR MR2007739 (2004m:20072)
- [20] Marston Conder, *Some results on quotients of triangle groups*, Bull. Austral. Math. Soc. **30** (1984), no. 1, 73–90. MR MR753563 (85j:20029)
- [21] ———, *The symmetric genus of alternating and symmetric groups*, J. Combin. Theory Ser. B **39** (1985), no. 2, 179–186. MR MR811121 (87e:20072)
- [22] ———, *A family of Hurwitz groups with nontrivial centres*, Bull. Austral. Math. Soc. **33** (1986), no. 1, 123–130. MR MR823860 (87e:20073b)
- [23] ———, *Hurwitz groups with arbitrarily large centres*, Bull. London Math. Soc. **18** (1986), no. 3, 269–271. MR MR829585 (87e:20073a)
- [24] ———, *Groups of minimal genus including  $C_2$  extensions of  $\text{PSL}(2, q)$  for certain  $q$* , Quart. J. Math. Oxford Ser. (2) **38** (1987), no. 152, 449–460. MR MR916227 (89a:20043)



- [25] ———, *Three-relator quotients of the modular group*, Quart. J. Math. Oxford Ser. (2) **38** (1987), no. 152, 427–447. MR MR916226 (88m:20069)
- [26] ———, *Maximal automorphism groups of symmetric Riemann surfaces with small genus*, J. Algebra **114** (1988), no. 1, 16–28. MR MR931896 (89c:20049)
- [27] ———, *A surprising isomorphism*, J. Algebra **129** (1990), no. 2, 494–501. MR MR1040950 (91f:20037)
- [28] ———, *A question by Graham Higman concerning quotients of the  $(2, 3, 7)$  triangle group*, J. Algebra **141** (1991), no. 2, 275–286. MR MR1125696 (92i:20034)
- [29] ———, *Two element generation of the finite reflection groups*, Quart. J. Math. Oxford Ser. (2) **46** (1995), no. 181, 95–106. MR MR1326134 (96c:20075)
- [30] Marston Conder, *Combinatorial and computational group-theoretic methods in the study of graphs, maps and polytopes with maximal symmetry*, Jack Koolen and Jin Ho Kwak and Ming-Yao Xu, Eds. Applications of Group Theory to Combinatorics, Taylor & Francis Group, London, 2008, pp. 1–11.
- [31] Marston Conder and Peter Dobcsányi, *Normal subgroups of the modular group and other Hecke groups*, Combinatorial group theory, discrete groups, and number theory, Contemp. Math., vol. 421, Amer. Math. Soc., Providence, RI, 2006, pp. 65–86. MR MR2303826
- [32] M. Cuntz and I. Heckenberger, *Finite Weyl groupoids of rank three*, 2009.
- [33] R. T. Curtis, *Symmetric presentations. I. Introduction, with particular reference to the Mathieu groups  $M_{12}$  and  $M_{24}$* , Groups, combinatorics & geometry (Durham, 1990), London Math. Soc. Lecture Note Ser., vol. 165, Cambridge Univ. Press, Cambridge, 1992, pp. 380–396. MR MR1200276 (94b:20038)
- [34] ———, *Symmetric presentations. II. The Janko group  $J_1$* , J. London Math. Soc. (2) **47** (1993), no. 2, 294–308. MR MR1207950 (94b:20039)
- [35] R. T. Curtis, A. M. A. Hammas, and J. N. Bray, *A systematic approach to symmetric presentations I: Involutory generators*, Math. Proc. Cambridge Philos. Soc. **119** (1996), no. 1, 23–34. MR MR1356154 (96k:20058)
- [36] B. de Smit and H. W. Lenstra, Jr., *Linearly equivalent actions of solvable groups*, J. Algebra **228** (2000), no. 1, 270–285. MR MR1760965 (2001f:20069)

- [37] Alberto L. Delgado, *Amalgams of type  $F_3$* , J. Algebra **117** (1988), no. 1, 149–161. MR MR955596 (89m:20032)
- [38] Marcus du Sautoy and Luke Woodward, *Nilpotent groups: Explicit examples*, Zeta Functions of Groups and Rings, Lecture Notes in Computer Science, vol. 1925/2008, Springer Berlin / Heidelberg, 2008, pp. 21–68.
- [39] Matthew J. Dyer, *Elementary roots and admissible subsets of coxeter groups*, J. Group Theory **To appear** (2009).
- [40] Bettina Eick and Delaram Kahrobaei, *Polycyclic groups: A new platform for cryptography?*, 2004.
- [41] Graham Ellis, *On groups with a finite nilpotent upper central quotient*, Arch. Math. (Basel) **70** (1998), no. 2, 89–96. MR MR1491453 (99a:20033)
- [42] ———, *On the relation between upper central quotients and lower central series of a group*, Trans. Amer. Math. Soc. **353** (2001), no. 10, 4219–4234 (electronic). MR MR1837229 (2002f:20043)
- [43] Graham Ellis and Irina Kholodna, *Three-dimensional presentations for the groups of order at most 30*, LMS J. Comput. Math. **2** (1999), 93–117+2 appendixes (HTML and source code) (electronic). MR MR1704216 (2000m:20048)
- [44] Pavel Etingof and Eric Rains, *New deformations of group algebras of Coxeter groups. II*, Geom. Funct. Anal. **17** (2008), no. 6, 1851–1871. MR MR2399085
- [45] Peter Fleischmann, *On pointwise conjugacy of distinguished coset representatives in Coxeter groups*, J. Group Theory **5** (2002), no. 3, 269–283. MR MR1914344 (2003f:20059)
- [46] Thomas A. Fournelle and Kenneth W. Weston, *Verbal embeddings and a geometric approach to some group presentations*, J. Algebra **124** (1989), no. 2, 300–316. MR MR1011596 (90g:20045)
- [47] ———, *A geometric approach to some group presentations*, Combinatorial Group Theory (College Park, MD, 1988), Contemp. Math., vol. 109, Amer. Math. Soc., Providence, RI, 1990, pp. 25–33. MR MR1076374 (91k:20023)

- [48] Volker Gebhardt, *Computer aided discovery of a fast algorithm for testing conjugacy in braid groups*, *Discovering Mathematics with Magma, Algorithms Comput. Math.*, vol. 19, Springer, Berlin, 2006, pp. 261–285. MR MR2278932
- [49] Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii, and Eugene Plotkin, *A description of Baer-Suzuki type of the solvable radical of a finite group*, *J. Pure Appl. Algebra* **213** (2009), no. 2, 250–258. MR MR2467402 (2009i:20045)
- [50] Fritz Grunewald and Alexander Lubotzky, *Linear representations of the automorphism group of a free group*, *Geometric and Functional Analysis* **18** (2010), no. 5, 1564–1608.
- [51] Simon Guest, *A solvable version of the Baer–Suzuki theorem*, *Trans. Amer. Math. Soc.* **362** (2010), 5909–5946. MR MR2661502
- [52] R. M. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky, *Remarks on proficient groups*, *J. Algebra* **326** (2011), no. 1, 169–184.
- [53] R. Haas and A. G. Helminck, *Algorithms for twisted involutions in Weyl groups*, 2006.
- [54] George Havas and Derek F. Holt, *On Coxeter’s families of group presentations*, *J. Algebra* **324** (2010), no. 5, 1076–1082. MR 2659213
- [55] George Havas, Derek F. Holt, P. E. Kenne, and Sarah Rees, *Some challenging group presentations*, *J. Austral. Math. Soc. Ser. A* **67** (1999), no. 2, 206–213. MR MR1717414 (2000h:20055)
- [56] George Havas, Derek F. Holt, and M. F. Newman, *Certain cyclically presented groups are infinite*, *Comm. Algebra* **29** (2001), no. 11, 5175–5178. MR MR1856948 (2002h:20046)
- [57] George Havas, M. F. Newman, Alice C. Niemeyer, and Charles C. Sims, *Groups with exponent six*, *Comm. Algebra* **27** (1999), no. 8, 3619–3638. MR MR1699578 (2000f:20049)
- [58] George Havas, M. F. Newman, and E. A. O’Brien, *Groups of deficiency zero*, *Geometric and Computational Perspectives on Infinite Groups (Minneapolis, MN and New Brunswick, NJ, 1994)*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 25, Amer. Math. Soc., Providence, RI, 1996, pp. 53–67. MR MR1364179 (96h:20063)

- [59] ———, *On the efficiency of some finite groups*, *Comm. Algebra* **32** (2004), no. 2, 649–656. MR MR2101831 (2005k:20078)
- [60] George Havas and Colin Ramsay, *Short balanced presentations of perfect groups*, *Groups St. Andrews 2001 in Oxford. Vol. I*, *London Math. Soc. Lecture Note Ser.*, vol. 304, Cambridge Univ. Press, Cambridge, 2003, pp. 238–243. MR MR2051529
- [61] ———, *On proofs in finitely presented groups*, *Groups St. Andrews 2005. Vol. 2*, *London Math. Soc. Lecture Note Ser.*, vol. 340, Cambridge Univ. Press, Cambridge, 2007, pp. 457–474. MR MR2331604 (2008f:20059)
- [62] George Havas, J. S. Richardson, and Leon S. Sterling, *The last of the Fibonacci groups*, *Proc. Roy. Soc. Edinburgh Sect. A* **83** (1979), no. 3-4, 199–203. MR MR549854 (82j:20068)
- [63] George Havas and Edmund F. Robertson, *Two groups which act on cubic graphs*, *Computational Group Theory (Durham, 1982)*, Academic Press, London, 1984, pp. 65–68. MR MR760650 (86b:05038)
- [64] ———, *Central factors of deficiency zero groups*, *Comm. Algebra* **24** (1996), no. 11, 3483–3487. MR MR1405266 (97e:20052)
- [65] George Havas, Edmund F. Robertson, and Dale C. Sutherland, *Behind and beyond a theorem on groups related to trivalent graphs*, *J. Aust. Math. Soc.* **85** (2008), no. 3, 323–332.
- [66] George Havas and M. R. Vaughan-Lee, *4-Engel groups are locally nilpotent*, *Internat. J. Algebra Comput.* **15** (2005), no. 4, 649–682. MR MR2160572 (2006d:20064)
- [67] ———, *Computing with 4-Engel groups*, *Groups St. Andrews 2005. Vol. 2*, *London Math. Soc. Lecture Note Ser.*, vol. 340, Cambridge Univ. Press, Cambridge, 2007, pp. 475–485. MR MR2331605 (2008e:20059)
- [68] George Havas and Michael Vaughan-Lee, *On counterexamples to the Hughes conjecture*, *J. Algebra* **322** (2009), no. 3, 791–801.
- [69] Derek F. Holt and Sarah Rees, *Computing with abelian sections of finitely presented groups*, *J. Algebra* **214** (1999), no. 2, 714–728. MR MR1680528 (2000b:20037)
- [70] Robert B. Howlett and Yunchuan Yin, *Computational construction of irreducible  $W$ -graphs for types  $E_6$  and  $E_7$* , *J. Algebra* **321** (2009), no. 8, 2055–2067. MR MR2501509

- [71] Mervyn C. Hughes and Alun O. Morris, *Root systems for two dimensional complex reflection groups*, Sémin. Lothar. Combin. **45** (2000/01), Art. B45e, 18 pp. (electronic). MR MR1816644 (2001k:20083)
- [72] Stephen P. Humphries, *Quotients of Coxeter complexes, fundamental groupoids and regular graphs*, Math. Z. **217** (1994), no. 2, 247–273. MR MR1296396 (95i:20059)
- [73] ———, *Action of braid groups on determinantal ideals, compact spaces and a stratification of Teichmüller space*, Invent. Math. **144** (2001), no. 3, 451–505. MR MR1833891 (2002c:20056)
- [74] ———, *Finite Hurwitz braid group actions on sequences of Euclidean reflections*, J. Algebra **269** (2003), no. 2, 556–588. MR MR2015854 (2005a:20055)
- [75] ———, *Finite Hurwitz braid group actions for Artin groups*, Israel J. Math. **143** (2004), 189–222. MR MR2106983 (2005i:20061)
- [76] ———, *Representations and rigidity of  $\text{Aut}(F_3)$* , Internat. J. Algebra Comput. **16** (2006), no. 5, 925–929. MR MR2274721
- [77] ———, *Subgroups of pure braid groups generated by powers of Dehn twists*, Rocky Mountain J. Math. **37** (2007), no. 3, 801–828. MR MR2351292
- [78] ———, *Subgroups of free groups generated by conjugates of powers of the generators*, J. Group Theory **12** (2009), no. 3, 465–485. MR MR2510210
- [79] Enrico Jabara, *Automorphisms with finite Reidemeister number in residually finite groups*, J. Algebra **320** (2008), no. 10, 3671–3679. MR MR2457715
- [80] Luise-Charlotte Kappe and Robert Fitzgerald Morse, *On commutators in groups*, Groups St. Andrews 2005. Vol. 2, London Math. Soc. Lecture Note Ser., vol. 340, Cambridge Univ. Press, Cambridge, 2007, pp. 531–558. MR MR2331612 (2008g:20068)
- [81] P. E. Kenne, *Presentations for some direct products of groups*, Bull. Austral. Math. Soc. **28** (1983), no. 1, 131–133. MR MR726809 (85a:20014)
- [82] ———, *Efficient presentations for three simple groups*, Comm. Algebra **14** (1986), no. 5, 797–800. MR MR834464 (87c:20060)

- [83] ———, *Some new efficient soluble groups*, *Comm. Algebra* **18** (1990), no. 8, 2747–2753. MR MR1074253 (91j:20081)
- [84] Jennifer D. Key and Johannes Siemons, *Regular sets and geometric groups*, *Results Math.* **11** (1987), no. 1-2, 97–116. MR MR880196 (88b:20062)
- [85] Anastasia V. Kisil, *Gromov conjecture on surface subgroups: Computational experiments*, 2010.
- [86] Peter Köhler, Thomas Meixner, and Michael Wester, *Triangle groups*, *Comm. Algebra* **12** (1984), no. 13-14, 1595–1625. MR MR743306 (86b:20047)
- [87] Joachim König, *Solvability of generalized monomial groups*, *J. Group Theory* **To appear** (2009).
- [88] Peter Lorimer, *Hyperbolic pyritohedra constructed from the Coxeter group [4, 3, 5]*, *Computational Algebra and Number Theory (Sydney, 1992)*, *Math. Appl.*, vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 303–321. MR MR1344939 (96d:20037)
- [89] Arturo Magidin, *Capability of nilpotent products of cyclic groups*, *J. Group Theory* **8** (2005), no. 4, 431–452. MR MR2152690 (2006c:20073)
- [90] Ivan Marin and Jean Michel, *Automorphisms of complex reflection groups*, 2007.
- [91] M. F. Newman, *On a family of cyclically-presented fundamental groups*, *J. Aust. Math. Soc.* **71** (2001), no. 2, 235–241, Special issue on group theory. MR MR1847194 (2002e:20067)
- [92] ———, *Automorphism groups of free groups*, *J. Aust. Math. Soc.* **85** (2008), no. 3, 341–345. MR MR2476444 (2009k:20080)
- [93] M. F. Newman and Michael Vaughan-Lee, *Engel-4 groups of exponent 5. II. Orders*, *Proc. London Math. Soc. (3)* **79** (1999), no. 2, 283–317. MR MR1702244 (2000e:20065)
- [94] Sarah B. Perkins and Peter J. Rowley, *Minimal and maximal length involutions in finite Coxeter groups*, *Comm. Algebra* **30** (2002), no. 3, 1273–1292. MR MR1892601 (2003b:20056)
- [95] ———, *On negative orbits of finite Coxeter groups*, *J. Algebraic Combin.* **20** (2004), no. 1, 17–31. MR MR2104818 (2005m:20091)

- [96] Norbert Peyerimhoff and Alina Vdovina, *Cayley graph expanders and groups of finite width*, 2008.
- [97] W. Plesken and A. Fabiańska, *An  $L_2$ -quotient algorithm for finitely presented groups*, J. Algebra **322** (2009), no. 3, 914–935. MR MR2531230
- [98] Evija Ribnere, *Sequences of words characterizing finite solvable groups*, Monatsh. Math **157** (2009), no. 4, 387–401.
- [99] Mark Sapir, *Residual properties of 1-relator groups*, 2010.
- [100] Neil Saunders, *Minimal faithful permutation degrees for irreducible Coxeter groups*, 2008.
- [101] Mohamed Sayed, *Nested symmetric representation of elements of the Suzuki chain groups*, Int. J. Math. Math. Sci. **2003** (2003), no. 62, 3931–3948. MR MR2036087 (2004m:20061)
- [102] Jian-Yi Shi, *Congruence classes of presentations for the complex reflection groups  $G(m, 1, n)$  and  $G(m, m, n)$* , Indag. Math. (N.S.) **16** (2005), no. 2, 267–288.
- [103] Pablo Spiga, *CI-property of elementary abelian 3-groups*, Discrete Math. **309** (2009), no. 10, 3393–3398. MR MR2526758
- [104] P. Christopher Staecker, *Computing twisted conjugacy classes in free groups using nilpotent quotients*, 2007.
- [105] ———, *Remnant properties in nielsen coincidence theory*, 2008.
- [106] John R. Stembridge, *Explicit matrices for irreducible representations of Weyl groups*, Represent. Theory **8** (2004), 267–289 (electronic). MR MR2077483 (2005h:20096)
- [107] Polina Strogova, *Finding a finite group presentation using rewriting*, Symbolic Rewriting Techniques (Ascona, 1995), Progr. Comput. Sci. Appl. Logic, vol. 15, Birkhäuser, Basel, 1998, pp. 267–276. MR MR1624600 (99d:20046)
- [108] G. Stroth and R. Weiss, *Groups with the BNB-property*, Geom. Dedicata **35** (1990), no. 1-3, 251–282. MR MR1066568 (91h:20058)
- [109] M. Chiara Tamburini and M. A. Vsemirnov, *Irreducible  $(237)$ -subgroups of  $n$ [less-than-or-equals slant] $7$  ii*, Journal of Algebra **To appear** (2009).

- [110] Stephen Tawn, *A presentation for the pure Hilden group*, 2009.
- [111] Michael Vaughan-Lee, *The restricted Burnside problem*, second ed., London Mathematical Society Monographs. New Series, vol. 8, The Clarendon Press Oxford University Press, New York, 1993. MR MR1364414 (98b:20047)
- [112] ———, *Engel-4 groups of exponent 5*, Proc. London Math. Soc. (3) **74** (1997), no. 2, 306–334. MR MR1425325 (98a:20036)
- [113] ———, *On 4-Engel groups*, LMS J. Comput. Math. **10** (2007), 341–353 (electronic). MR MR2342712
- [114] Christopher Voll, *Normal subgroup growth in free class-2-nilpotent groups*, Math. Ann. **332** (2005), no. 1, 67–79. MR MR2139251
- [115] M. Vsemirnov, *Groups  $G_2(p)$  as quotients of  $(2, 3, 7; 2p)$* , Transform. Groups **11** (2006), no. 2, 295–304. MR MR2231189
- [116] Richard Weiss, *A geometric characterization of the groups  $M_{12}$ , He and Ru*, J. Math. Soc. Japan **43** (1991), no. 4, 795–814. MR MR1126150 (92k:20076)
- [117] Uri Weiss, *On Shephard groups with large triangles*, 2009.
- [118] Gerald Williams, *The aspherical Cavicchioli-Hegenbarth-Pepovš generalized Fibonacci groups*, J. Group Theory **12** (2009), no. 1, 139–149. MR MR2488144 (2010c:20039)



# Linear Algebraic Groups

20Gxx

- [1] Maximilian Albert and Annette Maier, *Additive polynomials for finite groups of Lie type*, 2009.
- [2] Henrik Bäärnhielm, *Tensor decomposition of the Ree groups*, 2006.
- [3] László Babai and Robert Beals, *A polynomial-time theory of black box groups. I*, Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 30–64. MR MR1676609 (2000h:20089)
- [4] Tatiana Bandman, Fritz Grunewald, Boris Kunyavskii, and Nathan Jones, *Geometry and arithmetic of verbal dynamical systems on simple groups*, Groups, Geometry, and Dynamics **4** (2010), no. 4, 607–655.
- [5] C. Bates, D. Bundy, Sarah B. Perkins, and P. Rowley, *Commuting involution graphs in special linear groups*, Comm. Algebra **32** (2004), no. 11, 4179–4196. MR MR2102444 (2005g:20071)
- [6] C. P. Bendel, D. K. Nakano, B. J. Parshall, and C. Pillen, *Cohomology for quantum groups via the geometry of the Nullcone*, 2007, pp. 1–58.
- [7] Christopher P. Bendel, Daniel K. Nakano, and Cornelius Pillen, *Second cohomology groups for Frobenius kernels and related structures*, Adv. Math. **209** (2007), no. 1, 162–197. MR MR2294220 (2008c:20085)
- [8] John N. Bray, Derek F. Holt, and Colva M. Roney-Dougal, *Certain classical groups are not well-defined*, J. Group Theory **12** (2009), no. 2, 171–180. MR MR2502211
- [9] Peter A. Brooksbank, *Fast constructive recognition of black box symplectic groups*, J. Algebra **320** (2008), no. 2, 885–909. MR MR2422320
- [10] Donald I. Cartwright, *Groups acting simply transitively on the vertices of a building of type  $A_n$* , Groups of Lie Type and Their Geometries (Como, 1993), London Math. Soc. Lecture Note Ser., vol. 207, Cambridge Univ. Press, Cambridge, 1995, pp. 43–76. MR MR1320514 (96a:20039)

- [11] Donald I. Cartwright, Anna Maria Mantero, Tim Steger, and Anna Zappa, *Groups acting simply transitively on the vertices of a building of type  $A_2$ . I*, *Geom. Dedicata* **47** (1993), no. 2, 143–166. MR MR1232965 (95b:20053)
- [12] ———, *Groups acting simply transitively on the vertices of a building of type  $A_2$ . II. The cases  $q = 2$  and  $q = 3$* , *Geom. Dedicata* **47** (1993), no. 2, 167–223. MR MR1232966 (95b:20054)
- [13] Tracey Cicco, *Algorithms for Computing Restricted Root Systems and Weyl Groups*, PhD Thesis, North Carolina State University, 2006.
- [14] Arjeh M. Cohen and Scott H. Murray, *An algorithm for Lang’s Theorem*, *J. Algebra* **322** (2009), no. 3, 675–702. MR MR2531217
- [15] Marston Conder, Edmund Robertson, and Peter Williams, *Presentations for 3-dimensional special linear groups over integer rings*, *Proc. Amer. Math. Soc.* **115** (1992), no. 1, 19–26. MR MR1079696 (92h:20050)
- [16] Antonio Cossidente and Sam K. J. Vereecke, *Some geometry of the isomorphism  $\mathrm{Sp}(4, q) \cong \mathrm{O}(5, q)$ ,  $q$  even*, *J. Geom.* **70** (2001), no. 1-2, 28–37. MR MR1825542 (2002g:05043)
- [17] Willem A. de Graaf and Andrea Pavan, *Constructing arithmetic subgroups of unipotent groups*, *J. Algebra* **322** (2009), no. 11, 3950–3970. MR MR2556132
- [18] L. Di Martino, A. Previtali, and R. Radina, *Sets of transvections generating subgroups isomorphic to special linear groups*, *Comm. Algebra* **33** (2005), no. 6, 1663–1691. MR MR2150836 (2006c:20101)
- [19] Claus Fieker and Willem A. de Graaf, *Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras*, *LMS J. Comput. Math.* **10** (2007), 271–287 (electronic). MR MR2320832 (2008f:11119)
- [20] D. L. Flannery and E. A. O’Brien, *Linear groups of small degree over finite fields*, *Internat. J. Algebra Comput.* **15** (2005), no. 3, 467–502. MR MR2151423 (2006m:20075)
- [21] P. Fleischmann, W. Lempken, and A. E. Zalesskii, *Linear groups over  $\mathrm{GF}(2^k)$  generated by a conjugacy class of a fixed point free element of order 3*, *J. Algebra* **244** (2001), no. 2, 631–663. MR MR1859042 (2002i:20069)

- [22] Jason Fulman, *Random matrix theory over finite fields*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 1, 51–85 (electronic). MR MR1864086 (2002i:60012)
- [23] Skip Garibaldi and Michael Carr, *Geometries, the principle of duality, and algebraic groups*, Expo. Math. **24** (2006), no. 3, 195–234. MR MR2250947
- [24] Nikolai Gordeev, Fritz Grunewald, Boris Kunyavskii, and Eugene Plotkin, *A description of Baer-Suzuki type of the solvable radical of a finite group*, J. Pure Appl. Algebra **213** (2009), no. 2, 250–258. MR MR2467402 (2009i:20045)
- [25] Neil A. Gordon, Trevor M. Jarvis, and Ron Shaw, *Aspects of the linear groups  $GL(n, 2)$ ,  $n < 7$* , J. Combin. Math. Combin. Comput. **53** (2005), 13–31. MR MR2137833 (2006b:20073)
- [26] Neil A. Gordon, Guglielmo Lunardon, and Ron Shaw, *Linear sections of  $GL(4, 2)$* , Bull. Belg. Math. Soc. Simon Stevin **5** (1998), no. 2-3, 287–311, Finite geometry and combinatorics (Deinze, 1997). MR MR1630033 (99g:51008)
- [27] Jan E. Grabowski, *Examples of quantum cluster algebras associated to partial flag varieties*, J. Pure Appl. Algebra **To appear** (2010).
- [28] Jan E. Grabowski and Stéphane Launois, *Quantum cluster algebra structures on quantum Grassmannians and their quantum Schubert cells: The finite-type cases*, Int.Math.Res. Not **To appear** (2010).
- [29] Gerhard Grams, *Erzeugende und Relationen gewisser orthogonaler und symplektischer Gruppen über  $GF(2)$* , Mitt. Math. Sem. Giessen (1987), no. 183, 55–75. MR MR935088 (89c:20068)
- [30] Robert L. Griess, Jr. and A. J. E. Ryba, *Embeddings of  $SL(2, 27)$  in complex exceptional algebraic groups*, Michigan Math. J. **50** (2002), no. 1, 89–99. MR MR1897035 (2003e:20052)
- [31] Benedict H. Gross and Gabriele Nebe, *Globally maximal arithmetic groups*, J. Algebra **272** (2004), no. 2, 625–642. MR MR2028074 (2005b:20091)
- [32] Robert Guralnick and Susan Montgomery, *Frobenius-Schur indicators for subgroups and the Drinfeld double of Weyl groups*, Trans. Amer. Math. Soc. **361** (2009), no. 7, 3611–3632. MR MR2491893

- [33] Gerhard Hiss, *Hermitian function fields, classical unitals, and representations of 3-dimensional unitary groups*, Indag. Math. (N.S.) **15** (2004), no. 2, 223–243. MR MR2071863 (2005c:20080)
- [34] R. B. Howlett, L. J. Rylands, and D. E. Taylor, *Matrix generators for exceptional groups of Lie type*, J. Symbolic Comput. **31** (2001), no. 4, 429–445. MR MR1823074 (2002c:20078)
- [35] I. M. Isaacs and Dikran B. Karagueuzian, *Involutions and characters of upper triangular matrix groups*, Math. Comp. **74** (2005), no. 252, 2027–2033 (electronic). MR MR2164110
- [36] William M. Kantor and Ákos Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708, viii+168. MR MR1804385 (2001m:68066)
- [37] ———, *Computing with matrix groups*, Groups, combinatorics & geometry (Durham, 2001), World Sci. Publishing, River Edge, NJ, 2003, pp. 123–137. MR MR1994963 (2004k:20098)
- [38] P. H. Kropholler, S. Mohseni Rajaei, and J. Segal, *Invariant rings of orthogonal groups over  $\mathbf{F}_2$* , Glasg. Math. J. **47** (2005), no. 1, 7–54. MR MR2200953 (2006i:13009)
- [39] Larry Lambe and Bhama Srinivasan, *A computation of Green functions for some classical groups*, Comm. Algebra **18** (1990), no. 10, 3507–3545. MR MR1063992 (91i:20041)
- [40] C. R. Leedham-Green and E. A. O’Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881. MR MR2531225 (2010e:20075)
- [41] Dimitri Leemans and Laurence Vauthier, *An atlas of abstract regular polytopes for small groups*, Aequationes Math. **72** (2006), no. 3, 313–320. MR MR2282877
- [42] G. I. Lehrer, *The cohomology of the regular semisimple variety*, J. Algebra **199** (1998), no. 2, 666–689. MR MR1489931 (98k:20080)
- [43] W. Lempken, *Constructing  $J_4$  in  $\mathrm{GL}(1333, 11)$* , Comm. Algebra **21** (1993), no. 12, 4311–4351. MR MR1242834 (94i:20032)
- [44] Martin W. Liebeck and E. A. O’Brien, *Finding the characteristic of a group of Lie type*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 741–754. MR MR2352733 (2008i:20058)

- [45] Alexander Lubotzky and Igor Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363 (electronic). MR MR1815215 (2003d:60012)
- [46] Christopher Macmeikan, *Toral arrangements*, The COE Seminar on Mathematical Sciences 2004, Sem. Math. Sci., vol. 31, Keio Univ., Yokohama, 2004, pp. 37–54. MR MR2130506 (2005m:20116)
- [47] Alice C. Niemeyer and Cheryl E. Praeger, *A recognition algorithm for non-generic classical groups over finite fields*, J. Austral. Math. Soc. Ser. A **67** (1999), no. 2, 223–253, Group theory. MR MR1717416 (2000i:20080)
- [48] Wilhelm Plesken and Michael Pohst, *On maximal finite irreducible subgroups of  $GL(n, \mathbf{Z})$ . I. The five and seven dimensional cases*, Math. Comp. **31** (1977), no. 138, 536–551. MR MR0444789 (56 #3137a)
- [49] ———, *On maximal finite irreducible subgroups of  $GL(n, \mathbf{Z})$ . II. The six dimensional case*, Math. Comp. **31** (1977), no. 138, 552–573. MR MR0444790 (56 #3137b)
- [50] Cheryl E. Praeger, *Primitive prime divisor elements in finite classical groups*, Groups St. Andrews 1997 in Bath, II, London Math. Soc. Lecture Note Ser., vol. 261, Cambridge Univ. Press, Cambridge, 1999, pp. 605–623. MR MR1676657 (2000h:20090)
- [51] L. J. Rylands and D. E. Taylor, *Matrix generators for the orthogonal groups*, J. Symbolic Comput. **25** (1998), no. 3, 351–360. MR MR1615330 (99d:20078)
- [52] David I. Stewart, *The reductive subgroups of  $G_2$* , J. Group Theory **13** (2010), no. 1, 117–130.
- [53] Pham Huu Tiep and A. E. Zalesskii, *Some aspects of finite linear groups: a survey*, J. Math. Sci. (New York) **100** (2000), no. 1, 1893–1914, Algebra, 12. MR MR1774360 (2001f:20107)
- [54] M. Vsemirnov, *Hurwitz groups of intermediate rank*, LMS J. Comput. Math. **7** (2004), 300–336 (electronic). MR MR2118177 (2005j:20058)
- [55] M. A. Vsemirnov, *Is the group  $SL(6, \mathbf{Z})$   $(2, 3)$ -generated?*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **330** (2006), no. Vopr. Teor. Predst. Algebr. i Grupp. 13, 101–130, 272. MR MR2253569

- [56] ———, *On the  $(2, 3)$ -generation of matrix groups over the ring of integers*, *Algebra i Analiz* **19** (2007), no. 6, 22–58. MR MR2411638
- [57] Maxim Vsemirnov, *The group  $GL(6, Z)$  is  $(2, 3)$ -generated*, *J. Group Theory* **10** (2007), no. 4, 425–430. MR MR2334749

# Matrix Groups (not Linear Algebraic)

20Hxx

- [1] Emilio Bujalance, F. J. Cirre, and Marston Conder, *On full automorphism groups of Riemann surfaces*, J. Symbolic Comput. **24** (1997), 235–265.
- [2] ———, *On extendability of group actions on compact Riemann surfaces*, Trans. Amer. Math. Soc. **355** (2003), no. 4, 1537–1557 (electronic). MR MR1946404 (2003k:20079)
- [3] Emilio Bujalance and Marston Conder, *On cyclic groups of automorphisms of Riemann surfaces*, J. London Math. Soc. (2) **59** (1999), no. 2, 573–584. MR MR1709666 (2000g:20098)
- [4] Marston Conder, *The genus of compact Riemann surfaces with maximal automorphism group*, J. Algebra **108** (1987), no. 1, 204–247. MR MR887205 (88f:20063)
- [5] Marston Conder, C. Maclachlan, G. J. Martin, and E. A. O’Brien, *2-generator arithmetic Kleinian groups. III*, Math. Scand. **90** (2002), no. 2, 161–179. MR MR1895609 (2003b:20071)
- [6] A. S. Detinko and D. L. Flannery, *Algorithms for computing with nilpotent matrix groups over infinite domains*, J. Symbolic Comput. **43** (2008), no. 1, 8–26. MR MR2381967 (2008j:20156)
- [7] Rene P. Felix, *The finite quotient groups of the plane crystallographic group  $p6m$* , Matimyás Mat. (1989), no. 1, 39–49. MR MR1040006 (90m:20054)
- [8] D. L. Flannery, *Irreducible monomial linear groups of degree four over finite fields*, Internat. J. Algebra Comput. **14** (2004), no. 3, 253–294. MR MR2075154 (2005d:20094)
- [9] Derek F. Holt and E. A. O’Brien, *A computer-assisted analysis of some matrix groups*, J. Algebra **300** (2006), no. 1, 199–212. MR MR2228643
- [10] Stephen P. Humphries, *Some subgroups of  $SL(3, \mathbf{Z})$  generated by involutions*, Glasgow Math. J. **32** (1990), no. 2, 127–136. MR MR1058525
- [11] Sadok Kallel and Denis Sjerve, *On the group of automorphisms of cyclic covers of the Riemann sphere*, Math. Proc. Cambridge Philos. Soc. **138** (2005), no. 2, 267–287. MR MR2132169 (2006c:20106)

- [12] Markus Kirschmer, *Finite symplectic matrix groups*.
- [13] C. R. Leedham-Green and E. A. O'Brien, *Recognising tensor-induced matrix groups*, J. Algebra **253** (2002), no. 1, 14–30. MR MR1925006 (2003g:20089)
- [14] Coy L. May and Jay Zimmerman, *The groups of symmetric genus  $\sigma \leq 8$* , Comm. Algebra **36** (2008), no. 11, 4078–4095. MR MR2460404 (2009i:14038)
- [15] Gabriele Nebe, *Finite quaternionic matrix groups*, Represent. Theory **2** (1998), 106–223 (electronic). MR MR1615333 (99f:20085)
- [16] J. Opgenorth, W. Plesken, and T. Schulz, *Crystallographic algorithms and tables*, Acta Cryst. Sect. A **54** (1998), no. 5, 517–531. MR MR1645546 (99h:20082)
- [17] Kathleen L. Petersen, *One-cusped congruence subgroups of Bianchi groups*, Math. Ann. **338** (2007), no. 2, 249–282. MR MR2302062 (2008b:20063)
- [18] W. Plesken and D. Robertz, *Representations, commutative algebra, and Hurwitz groups*, J. Algebra **300** (2006), no. 1, 223–247. MR MR2228645
- [19] Wilhelm Plesken and Tilman Schulz, *Counting crystallographic groups in low dimensions*, Experiment. Math. **9** (2000), no. 3, 407–411. MR MR1795312
- [20] Gerhard Rosenberger, *Von Untergruppen der Triangel-Gruppen*, Illinois J. Math. **22** (1978), no. 3, 404–413. MR MR497484 (81g:20092)
- [21] Alexander Stein, *On Bruck loops of 2-power exponent, II*, 2009.
- [22] M. Chiara Tamburini and M. Vsemirnov, *Irreducible  $(2, 3, 7)$ -subgroups of  $\mathrm{PGL}_n(\mathbf{F})$ ,  $n \leq 7$* , J. Algebra **300** (2006), no. 1, 339–362. MR MR2228652
- [23] John Voight, *Computing fundamental domains for Fuchsian groups*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 469–491. MR MR2541438
- [24] Reza Zomorrodian, *On a theorem of supersoluble automorphism groups*, Proc. Amer. Math. Soc. **131** (2003), no. 9, 2711–2713 (electronic). MR MR1974326 (2004d:20060)



# Cohomology

20Jxx

- [1] A. Adem, J. F. Carlson, D. B. Karagueuzian, and R. James Milgram, *The cohomology of the Sylow 2-subgroup of the Higman-Sims group*, J. Pure Appl. Algebra **164** (2001), no. 3, 275–305. MR MR1857743 (2002g:20089)
- [2] Alejandro Adem, *Recent developments in the cohomology of finite groups*, Notices Amer. Math. Soc. **44** (1997), no. 7, 806–812. MR MR1460209 (98j:20077)
- [3] Alejandro Adem, Dikran Karagueuzian, R. James Milgram, and Kristin Umland, *The cohomology of the Lyons group and double covers of alternating groups*, J. Algebra **208** (1998), no. 2, 452–479. MR MR1655462 (99m:20128)
- [4] Dave Benson, *Dickson invariants, regularity and computation in group cohomology*, Illinois J. Math. **48** (2004), no. 1, 171–197. MR MR2048221 (2005c:20089)
- [5] Inger Christin Borge, *A cohomological approach to the classification of  $p$ -groups*, Ph.D. thesis, University of Oxford, 2001.
- [6] John N. Bray and Robert A. Wilson, *Examples of 3-dimensional 1-cohomology for absolutely irreducible modules of finite simple groups*, J. Group Theory **11** (2008), no. 5, 669–673. MR MR2446148
- [7] Jon F. Carlson, *Problems in the calculation of group cohomology*, Computational Methods for Representations of Groups and Algebras (Essen, 1997), Progr. Math., vol. 173, Birkhäuser, Basel, 1999, pp. 107–120. MR MR1714605 (2001i:20111)
- [8] ———, *Calculating group cohomology: Tests for completion*, J. Symbolic Comput. **31** (2001), no. 1-2, 229–242, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806218 (2002c:20083)
- [9] ———, *Coclass and cohomology*, J. Pure Appl. Algebra **200** (2005), no. 3, 251–266. MR MR2147269
- [10] ———, *Cohomology, computations, and commutative algebra*, Notices Amer. Math. Soc. **52** (2005), no. 4, 426–434. MR MR2127572 (2006f:20061)

- [11] Jon F. Carlson, Edward L. Green, and Gerhard J. A. Schrieder, *Computing Ext algebras for finite groups*, J. Symbolic Comput. **24** (1997), no. 3-4, 317–325, Computational algebra and number theory (London, 1993). MR MR1484482 (98k:20086)
- [12] Jon F. Carlson, John S. Maginnis, and R. James Milgram, *The cohomology of the sporadic groups  $J_2$  and  $J_3$* , J. Algebra **214** (1999), no. 1, 143–173. MR MR1684888 (2000a:20116)
- [13] Jon F. Carlson, Lisa Townsley, Luis Valeri-Elizondo, and Mucheng Zhang, *Cohomology Rings of Finite Groups*, Algebras and Applications, vol. 3, Kluwer Academic Publishers, Dordrecht, 2003, With an appendix: Calculations of cohomology rings of groups of order dividing 64 by Carlson, Valeri-Elizondo and Zhang. MR MR2028960 (2004k:20110)
- [14] Graham Ellis and Irina Kholodna, *Computing second cohomology of finite groups with trivial coefficients*, Homology Homotopy Appl. **1** (1999), 163–168 (electronic). MR MR1796417 (2001k:20115)
- [15] Graham Ellis and Frank Leonard, *Computing Schur multipliers and tensor products of finite groups*, Proc. Roy. Irish Acad. Sect. A **95** (1995), no. 2, 137–147. MR MR1660373 (99h:20084)
- [16] D. L. Flannery, *Cocyclic Hadamard matrices and Hadamard groups are equivalent*, J. Algebra **192** (1997), no. 2, 749–779. MR MR1452686 (98f:20036)
- [17] D. L. Flannery and E. A. O’Brien, *Computing 2-cocycles for central extensions and relative difference sets*, Comm. Algebra **28** (2000), no. 4, 1939–1955. MR MR1747364 (2001a:20090)
- [18] David J. Green, *Gröbner Bases and the Computation of Group Cohomology*, Lecture Notes in Mathematics, vol. 1828, Springer-Verlag, Berlin, 2003. MR MR2032182 (2005d:20096)
- [19] Derek F. Holt, *Cohomology and group extensions in Magma*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 221–241. MR MR2278930
- [20] Alain LeBel, D. L. Flannery, and K. J. Horadam, *Group algebra series and coboundary modules*, J. Pure Appl. Algebra **214** (2010), no. 7, 1291–1300. MR 2587004 (2011b:20011)

- [21] Yujie Ma, *Cohomology of special 128-groups*, 1999.
- [22] John Martino and Stewart Priddy, *Group extensions and automorphism group rings*, *Homology Homotopy Appl.* **5** (2003), no. 1, 53–70 (electronic). MR MR1989613 (2004e:20091)

# Loops, Quasigroups and Semigroups

20Mxx, 20Nxx

- [1] J. Araújo, P. V. Bünaeu, J. D. Mitchell, and M. Neunhöffer, *Computing automorphisms of semigroups*, J. Symbolic Comput. **45** (2010), no. 3, 373–392. MR MR2578344
- [2] João Araújo and Csaba Schneider, *The rank of the endomorphism monoid of a uniform partition*, Semigroup Forum **78** (2009), no. 3, 498–510. MR MR2511780
- [3] Tuval Foguel, *Groups, transversals, and loops*, Comment. Math. Univ. Carolin. **41** (2000), no. 2, 261–269, Loops’99 (Prague). MR MR1780870 (2001h:20099)
- [4] Tuval Foguel and Abraham A. Ungar, *Involutory decomposition of groups into twisted subgroups and subgroups*, J. Group Theory **3** (2000), no. 1, 27–46. MR MR1736515 (2001f:20144)
- [5] ———, *Gyrogroups and the decomposition of groups into twisted subgroups and subgroups*, Pacific J. Math. **197** (2001), no. 1, 1–11. MR MR1810204 (2002e:20142)
- [6] Andrei Kelarev, *Graph algebras and automata*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 257, Marcel Dekker Inc., New York, 2003. MR MR2064147 (2005e:68001)
- [7] Kenneth Kunen, *G-loops and permutation groups*, J. Algebra **220** (1999), no. 2, 694–708. MR MR1717366 (2000j:20133)
- [8] Sasha Rubin, *Automata presenting structures: a survey of the finite string case*, Bull. Symbolic Logic **14** (2008), no. 2, 169–209. MR MR2413002

# Computational Group Theory

20-04

- [1] Sophie Ambrose, *Matrix Groups: Theory, Algorithms and Applications*, PhD Thesis, University of Western Australia, 2005, p. 167.
- [2] Sophie Ambrose, Max Neunhöffer, Cheryl E. Praeger, and Csaba Schneider, *Generalised sifting in black-box groups*, LMS J. Comput. Math. **8** (2005), 217–250 (electronic). MR MR2193212 (2006m:20001)
- [3] Henrik Bäärnhielm, *Recognising the Ree groups in their natural representations*, 2006.
- [4] ———, *Tensor decomposition of the Ree groups*, 2006.
- [5] Henrik Bäärnhielm, *Algorithmic problems in twisted groups of Lie type*, 2008.
- [6] László Babai and Robert Beals, *A polynomial-time theory of black box groups. I*, Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 30–64. MR MR1676609 (2000h:20089)
- [7] László Babai and Igor Pak, *Strong bias of group generators: An obstacle to the “product replacement algorithm”*, J. Algorithms **50** (2004), no. 2, 215–231, SODA 2000 special issue. MR MR2053017 (2005b:60012)
- [8] Hans Ulrich Besche and Bettina Eick, *The groups of order at most 1000 except 512 and 768*, J. Symbolic Comput. **27** (1999), no. 4, 405–413. MR MR1681347 (2000c:20002)
- [9] Hans Ulrich Besche, Bettina Eick, and E. A. O’Brien, *The groups of order at most 2000*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 1–4 (electronic). MR MR1826989
- [10] ———, *A millennium project: Constructing small groups*, Internat. J. Algebra Comput. **12** (2002), no. 5, 623–644. MR MR1935567 (2003h:20042)
- [11] Alexandre V. Borovik, *Centralisers of involutions in black box groups*, Computational and Statistical Group Theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 7–20. MR MR1929713 (2003i:60010)

- [12] J. D. Bradley and R. T. Curtis, *Symmetric generation and existence of  $\text{McL} : 2$ , the automorphism group of the McLaughlin group*, *Comm. Algebra* **38** (2010), no. 2, 601–617. MR 2598901
- [13] John Bray, Marston Conder, Charles Leedham-Green, and Eamonn O’Brien, *Short presentations for alternating and symmetric groups*, 2006.
- [14] John N. Bray and Robert T. Curtis, *Double coset enumeration of symmetrically generated groups*, *J. Group Theory* **7** (2004), no. 2, 167–185. MR MR2049015 (2005b:20059)
- [15] Peter A. Brooksbank and William M. Kantor, *Fast constructive recognition of black box orthogonal groups*, *J. Algebra* **300** (2006), no. 1, 256–288. MR MR2228648
- [16] Peter A. Brooksbank and E. A. O’Brien, *On intersections of classical groups*, *J. Group Theory* **11** (2008), no. 4, 465–478. MR MR2429348
- [17] Ronald Brown, Neil Ghani, Anne Heyworth, and Christopher D. Wensley, *String rewriting for double coset systems*, *J. Symbolic Comput.* **41** (2006), no. 5, 573–590. MR MR2209165 (2006m:20044)
- [18] Timothy C. Burness, Martin W. Liebeck, and Aner Shalev, *Base sizes for simple groups and a conjecture of Cameron*, *Proc. Lond. Math. Soc. (3)* **98** (2009), no. 1, 116–162. MR MR2472163 (2009m:20001)
- [19] Timothy C. Burness, E. A. O’Brien, and Robert A. Wilson, *Base sizes for sporadic simple groups*, 2008.
- [20] G. Butler, S. S. Iyer, and E. A. O’Brien, *A database of groups of prime-power order*, *Softw., Pract. Exper.* **24** (1994), no. 10, 911–951 (English).
- [21] Colin M. Campbell, George Havas, and Edmund F. Robertson, *Addendum to: “An elementary introduction to coset table methods in computational group theory”*, *Groups—St. Andrews 1981*, *London Math. Soc. Lecture Note Ser.*, vol. 71, Cambridge Univ. Press, Cambridge, 2007, pp. 361–364. MR MR2352804
- [22] John Cannon and George Havas, *Algorithms for groups*, *Australian Computer Journal* **24** (1992), 51–60.

- [23] John Cannon and Bernd Souvignier, *On the computation of conjugacy classes in permutation groups*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Kihei, HI) (New York), ACM, 1997, pp. 392–399 (electronic). MR MR1810005
- [24] John J. Cannon, Bruce C. Cox, and Derek F. Holt, *Computing Sylow subgroups in permutation groups*, J. Symbolic Comput. **24** (1997), no. 3-4, 303–316, Computational algebra and number theory (London, 1993). MR MR1484481 (98m:20010)
- [25] ———, *Computing the subgroups of a permutation group*, J. Symbolic Comput. **31** (2001), no. 1-2, 149–161, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806212 (2002e:20008)
- [26] John J. Cannon, Bettina Eick, and Charles R. Leedham-Green, *Special polycyclic generating sequences for finite soluble groups*, J. Symbolic Comput. **38** (2004), no. 5, 1445–1460. MR MR2168723
- [27] John J. Cannon and Derek F. Holt, *Computing chief series, composition series and socles in large permutation groups*, J. Symbolic Comput. **24** (1997), no. 3-4, 285–301, Computational algebra and number theory (London, 1993). MR MR1484480 (98m:20009)
- [28] ———, *Automorphism group computation and isomorphism testing in finite groups*, J. Symbolic Comput. **35** (2003), no. 3, 241–267. MR MR1962794 (2004c:20035)
- [29] ———, *Computing conjugacy class representatives in permutation groups*, J. Algebra **300** (2006), no. 1, 213–222. MR MR2228644 (2007f:20002)
- [30] John J. Cannon, Derek F. Holt, Michael Slattery, and Allan K. Steel, *Computing subgroups of bounded index in a finite group*, J. Symbol. Comput. **40** (2005), no. 2, 1013–1022. MR MR2167681 (2006k:20007)
- [31] Bill Casselman, *Computation in Coxeter groups. II. Constructing minimal roots*, Represent. Theory **12** (2008), 260–293. MR MR2439007
- [32] Frank Celler, Charles R. Leedham-Green, Scott H. Murray, Alice C. Niemeyer, and E. A. O’Brien, *Generating random elements of a finite group*, Comm. Algebra **23** (1995), no. 13, 4931–4948. MR MR1356111 (96h:20115)
- [33] Arjeh M. Cohen, Sergei Haller, and Scott H. Murray, *Computing in unipotent and reductive algebraic groups*, LMS J. Comput. Math. **11** (2008), 343–366. MR MR2452553

- [34] ———, *Computing with root subgroups of twisted reductive groups*, 2009.
- [35] Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, *Math. Comp.* **73** (2004), no. 247, 1477–1498 (electronic). MR MR2047097 (2005a:20068)
- [36] Marston Conder, *Experimental algebra*, *Math. Chronicle* **20** (1991), 1–11. MR MR1137869 (92k:20007)
- [37] Marston Conder and Peter Dobcsányi, *Applications and adaptations of the low index subgroups procedure*, *Math. Comp.* **74** (2005), no. 249, 485–497 (electronic). MR MR2085903 (2005e:20046)
- [38] Marston Conder, C. R. Leedham-Green, and E. A. O’Brien, *Constructive recognition of  $\text{PSL}(2, q)$* , *Trans. Amer. Math. Soc.* **358** (2006), no. 3, 1203–1221 (electronic). MR MR2187651 (2006j:20017)
- [39] Marston Conder and Charles R. Leedham-Green, *Fast recognition of classical groups over large fields*, *Groups and Computation III* (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 113–121. MR MR1829474 (2002g:20001)
- [40] Gene Cooperman, Larry Finkelstein, and Michael Tselman, *Computing with matrix groups using permutation representations*, *ISSAC '95: Proceedings of the 1995 international symposium on Symbolic and algebraic computation* (New York, NY, USA), ACM Press, 1995, pp. 259–264.
- [41] Gene Cooperman, Larry Finkelstein, Michael Tselman, and Bryant York, *Constructing permutation representations for matrix groups*, *J. Symbolic Comput.* **24** (1997), no. 3-4, 471–488, *Computational algebra and number theory* (London, 1993). MR MR1484493 (98h:20090)
- [42] Gene Cooperman and Eric Robinson, *Memory-based and disk-based algorithms for very high degree permutation groups*, *ISSAC '03: Proceedings of the 2003 international symposium on Symbolic and algebraic computation* (New York, NY, USA), ACM Press, 2003, pp. 66–73.
- [43] A. S. Detinko and D. L. Flannery, *On deciding finiteness of matrix groups*, *J. Symbolic Comput.* **44** (2009), no. 8, 1037–1043. MR MR2523766



- [44] A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Deciding finiteness of matrix groups in positive characteristic*, *J. Algebra* **322** (2009), no. 11, 4151–4160. MR MR2556145
- [45] Fokko du Cloux, *The state of the art in the computation of Kazhdan-Lusztig polynomials*, *Appl. Algebra Engrg. Comm. Comput.* **7** (1996), no. 3, 211–219.
- [46] Bettina Eick, *Computational group theory*, Jahresber. Deutsch. Math.-Verein. **107** (2005), no. 3, 155–170. MR MR2173979 (2006h:20001)
- [47] Bettina Eick, C. R. Leedham-Green, and E. A. O'Brien, *Constructing automorphism groups of  $p$ -groups*, *Comm. Algebra* **30** (2002), no. 5, 2271–2295. MR MR1904637 (2003d:20027)
- [48] Bettina Eick and E. A. O'Brien, *Enumerating  $p$ -groups*, *J. Austral. Math. Soc. Ser. A* **67** (1999), no. 2, 191–205, Group theory. MR MR1717413 (2000h:20033)
- [49] Arash Farzan and J. Ian Munro, *Succinct representation of finite abelian groups*, ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 2006, pp. 87–92.
- [50] Claus Fieker, *Minimizing representations over number fields*, *J. Symbolic Comput.* **38** (2004), no. 1, 833–842. MR MR2094558 (2005g:20023)
- [51] Claus Fieker and Jürgen Klüners, *Minimal discriminants for fields with small Frobenius groups as Galois groups*, *J. Number Theory* **99** (2003), no. 2, 318–337. MR MR1968456 (2004f:11147)
- [52] Volker Gebhardt, *Constructing a short defining set of relations for a finite group*, *J. Algebra* **233** (2000), no. 2, 526–542. MR MR1793915 (2001k:20065)
- [53] ———, *Efficient collection in infinite polycyclic groups*, *J. Symbolic Comput.* **34** (2002), no. 3, 213–228. MR MR1935079 (2003g:20001)
- [54] ———, *A new approach to the conjugacy problem in Garside groups*, *J. Algebra* **292** (2005), no. 1, 282–302. MR MR2166805
- [55] ———, *Conjugacy search in braid groups: From a braid-based cryptography point of view*, *Appl. Algebra Engrg. Comm. Comput.* **17** (2006), no. 3-4, 219–238. MR MR2233783

- [56] S. P. Glasby, C. R. Leedham-Green, and E. A. O'Brien, *Writing projective representations over subfields*, J. Algebra **295** (2006), no. 1, 51–61. MR MR2188850 (2006h:20002)
- [57] S.P. Glasby and Cheryl E. Praeger, *Towards an efficient Meat-axe algorithm using  $f$ -cyclic matrices: The density of unicyclic matrices in  $M(n, q)$* , J. Algebra **322** (2009), no. 3, 766–790.
- [58] Anja Groch, Dennis Hofheinz, and Rainer Steinwandt, *A practical attack on the root problem in braid groups*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 121–131. MR MR2389293
- [59] R. Haas and A. G. Helminck, *Algorithms for twisted involutions in Weyl groups*, 2006.
- [60] George Havas, *Coset enumeration strategies*, Watt, Stephen M. (ed.), ISSAC '91. Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation. Bonn, Germany, July 15–17, 1991. New York, NY: ACM Press, 1991, pp. 191–199.
- [61] George Havas, C. R. Leedham-Green, E. A. O'Brien, and Michael C. Slattery, *Computing with elation groups*, Finite Geometries, Groups, and Computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 95–102. MR MR2258003 (2007f:20003)
- [62] George Havas, M. F. Newman, Alice C. Niemeyer, and Charles C. Sims, *Computing in groups with exponent six*, Computational and Geometric Aspects of Modern Algebra, London Math. Soc. Lecture Note Ser., vol. 275, Cambridge Univ. Press, Cambridge, 1998, pp. 87–100.
- [63] George Havas and Colin Ramsay, *Proving a group trivial made easy: A case study in coset enumeration*, Bull. Austral. Math. Soc. **62** (2000), no. 1, 105–118. MR MR1775892 (2002j:20061)
- [64] ———, *On proofs in finitely presented groups*, Groups St. Andrews 2005. Vol. 2, London Math. Soc. Lecture Note Ser., vol. 340, Cambridge Univ. Press, Cambridge, 2007, pp. 457–474. MR MR2331604 (2008f:20059)
- [65] George Havas and Edmund F. Robertson, *Application of computational tools for finitely presented groups*, Computational support for discrete mathematics (Piscat-

- away, NJ, 1992), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 15, Amer. Math. Soc., Providence, RI, 1994, pp. 29–39. MR MR1281812 (95g:20001)
- [66] George Havas, Edmund F. Robertson, and Dale C. Sutherland, *Behind and beyond a theorem on groups related to trivalent graphs*, J. Aust. Math. Soc. **85** (2008), no. 3, 323–332.
- [67] George Havas and M. R. Vaughan-Lee, *Computing with 4-Engel groups*, Groups St. Andrews 2005. Vol. 2, London Math. Soc. Lecture Note Ser., vol. 340, Cambridge Univ. Press, Cambridge, 2007, pp. 475–485. MR MR2331605 (2008e:20059)
- [68] George Havas and Michael Vaughan-Lee, *On counterexamples to the Hughes conjecture*, J. Algebra **322** (2009), no. 3, 791–801.
- [69] P. E. Holmes, S. A. Linton, E. A. O’Brien, A. J. E. Ryba, and R. A. Wilson, *Constructive membership in black-box groups*, J. Group Theory **11** (2008), no. 6, 747–763. MR MR2466905
- [70] D. F. Holt, *The computation of normalizers in permutation groups*, J. Symbolic Comput. **12** (1991), no. 4-5, 499–516, Computational group theory, Part 2. MR MR1146513 (93b:20010)
- [71] Derek F. Holt, *The Meataxe as a tool in computational group theory*, The Atlas of Finite Groups: Ten Years On (Birmingham, 1995), London Math. Soc. Lecture Note Ser., vol. 249, Cambridge Univ. Press, Cambridge, 1998, pp. 74–81. MR MR1647414 (99k:20001)
- [72] ———, *Computing automorphism groups of finite groups*, Groups and Computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 201–208. MR MR1829481 (2002d:20033)
- [73] ———, *Cohomology and group extensions in Magma*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 221–241. MR MR2278930
- [74] Derek F. Holt, Bettina Eick, and Eamonn A. O’Brien, *Handbook of Computational Group Theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005. MR MR2129747 (2006f:20001)

- [75] Derek F. Holt, C. R. Leedham-Green, E. A. O'Brien, and Sarah Rees, *Computing matrix group decompositions with respect to a normal subgroup*, J. Algebra **184** (1996), no. 3, 818–838. MR MR1407872 (97m:20021)
- [76] ———, *Testing matrix groups for primitivity*, J. Algebra **184** (1996), no. 3, 795–817. MR MR1407871 (97m:20020)
- [77] Derek F. Holt and E. A. O'Brien, *A computer-assisted analysis of some matrix groups*, J. Algebra **300** (2006), no. 1, 199–212. MR MR2228643
- [78] Derek F. Holt and Mark J. Stather, *Computing a chief series and the soluble radical of a matrix group over a finite field*, LMS J. Comput. Math. **11** (2008), 223–251. MR MR2429998
- [79] Alexander Hulpke, *Computing subgroups invariant under a set of automorphisms*, J. Symbolic Comput. **27** (1999), no. 4, 415–427. MR MR1681348 (2000a:20001)
- [80] ———, *Representing subgroups of finitely presented groups by quotient subgroups*, Experiment. Math. **10** (2001), no. 3, 369–381. MR MR1917425 (2003i:20049)
- [81] ———, *Constructing transitive permutation groups*, J. Symbolic Comput. **39** (2005), no. 1, 1–30. MR MR2168238
- [82] Stephen P. Humphries, *Generators for the mapping class group*, Topology of low-dimensional manifolds (Proc. Second Sussex Conf., Chelwood Gate, 1977), Lecture Notes in Math., vol. 722, Springer, Berlin, 1979, pp. 44–47. MR 547453 (80i:57010)
- [83] Stephen P. Humphries and Kenneth W. Johnson, *Fusions of character tables II.  $p$ -groups*, Comm. Algebra **37** (2009), no. 12, 4296–4315. MR 2588851 (2010m:20011)
- [84] William M. Kantor, *Sylow's theorem in polynomial time*, J. Comput. System Sci. **30** (1985), no. 3, 359–394. MR MR805654 (87j:68064)
- [85] ———, *Simple groups in computational group theory*, Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), no. Extra Vol. II, 1998, pp. 77–86 (electronic). MR MR1648058 (99h:20002)
- [86] William M. Kantor and Ákos Seress, *Black box classical groups*, Mem. Amer. Math. Soc. **149** (2001), no. 708, viii+168. MR MR1804385 (2001m:68066)

- [87] Boris Kunyavskii, Eugene Plotkin, and Roman Shklyar, *A strategy for human-computer study of equations and identities in finite groups*, Proc. Latv. Acad. Sci. Sect. B Nat. Exact Appl. Sci. **57** (2003), no. 3-4, 97–101. MR MR2016269
- [88] Rudolf Land, *Computation of Pólya polynomials of primitive permutation groups*, Math. Comp. **36** (1981), no. 153, 267–278. MR MR595061 (82c:20010)
- [89] R. Laue, *Construction of groups and the constructive approach to group actions*, Symmetry and Structural Properties of Condensed Matter (Zajolhk Aczkowo, 1994), World Sci. Publishing, River Edge, NJ, 1995, pp. 404–416. MR MR1475245 (98m:20006)
- [90] Reinhard Laue, *Computing double coset representatives for the generation of solvable groups*, Computer algebra (Marseille, 1982), Lecture Notes in Comput. Sci., vol. 144, Springer, Berlin, 1982, pp. 65–70. MR MR680055 (83m:20005)
- [91] C. R. Leedham-Green and Scott H. Murray, *Variants of product replacement*, Computational and Statistical Group Theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 97–104. MR MR1929718 (2003h:20003)
- [92] C. R. Leedham-Green and E. A. O’Brien, *Recognising tensor-induced matrix groups*, J. Algebra **253** (2002), no. 1, 14–30. MR MR1925006 (2003g:20089)
- [93] ———, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), no. 3, 833–881. MR MR2531225 (2010e:20075)
- [94] Charles R. Leedham-Green, *The computational matrix group project*, Groups and Computation III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 229–247. MR MR1829483 (2002d:20084)
- [95] Martin W. Liebeck and E. A. O’Brien, *Finding the characteristic of a group of Lie type*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 741–754. MR MR2352733 (2008i:20058)
- [96] Eddie H. Lo, *A polycyclic quotient algorithm*, J. Symbolic Comput. **25** (1998), no. 1, 61–97. MR MR1600618 (99c:20040)
- [97] Andrea Lucchini and Federico Menegazzo, *Computing a set of generators of minimal cardinality in a solvable group*, J. Symbolic Comput. **17** (1994), no. 5, 409–420. MR MR1289999 (95e:20030)

- [98] Eugene M. Luks and Pierre McKenzie, *Parallel algorithms for solvable permutation groups*, J. Comput. System Sci. **37** (1988), no. 1, 39–62, 26th IEEE Conference on Foundations of Computer Science (Portland, OR, 1985). MR MR973656 (90f:68094)
- [99] Eugene M. Luks and Takunari Miyazaki, *Polynomial-time normalizers for permutation groups with restricted composition factors*, ISSAC '02: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (New York), ACM, 2002, pp. 176–183 (electronic). MR MR2035247 (2005d:20006)
- [100] Eugene M. Luks, Ferenc Rákóczi, and Charles R. B. Wright, *Computing normalizers in permutation  $p$ -groups*, ISSAC '94: Proceedings of the international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 1994, pp. 139–146.
- [101] Eugene M. Luks, Ferenc Rákóczi, and Charles R. B. Wright, *Some algorithms for nilpotent permutation groups*, J. Symbolic Comput. **23** (1997), no. 4, 335–354. MR MR1445430 (97m:68113)
- [102] Klaus M. Lux and Magdolna Szőke, *Computing homomorphism spaces between modules over finite dimensional algebras*, Experiment. Math. **12** (2003), no. 1, 91–98. MR MR2002676
- [103] Kay Magaard, Sergey Shpectorov, and Helmut Völklein, *A GAP package for braid orbit computation and applications*, Experiment. Math. **12** (2003), no. 4, 385–393. MR MR2043989 (2005e:12007)
- [104] Gerhard O. Michler, *An algorithm for determining the simplicity of a modular group representation*, J. Symbolic Comput. **6** (1988), no. 1, 105–111. MR MR961374 (89h:20013)
- [105] ———, *Some problems in computational representation theory*, J. Symbolic Comput. **9** (1990), no. 5-6, 571–582, Computational group theory, Part 1. MR MR1075423 (91k:20022)
- [106] Torsten Minkwitz, *On the computation of ordinary irreducible representations of finite groups*, ISSAC '95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 1995, pp. 278–284.
- [107] Takunari Miyazaki, *Polynomial-time computation in matrix groups*, PhD Thesis, University of Oregon, 1999.

- [108] Meinard Müller and Michael Clausen, *DFT-based word normalization in finite supersolvable groups*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 3-4, 213–231. MR MR2104296 (2005i:20055)
- [109] Scott H. Murray and E. A. O’Brien, *Selecting base points for the Schreier-Sims algorithm for matrix groups*, J. Symbolic Comput. **19** (1995), no. 6, 577–584. MR MR1370623 (97c:20003)
- [110] J. Neubüser, *An invitation to computational group theory*, Groups ’93 Galway/St. Andrews, Vol. 2, London Math. Soc. Lecture Note Ser., vol. 212, Cambridge Univ. Press, Cambridge, 1995, pp. 457–475. MR MR1337288 (96c:20002)
- [111] Peter M. Neumann and Cheryl E. Praeger, *Cyclic matrices and the MEATAXE*, Groups and Computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 291–300. MR MR1829488 (2002d:20018)
- [112] Max Neunhöffer and Ákos Seress, *A data structure for a uniform approach to computations with finite groups*, ISSAC’06: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2006, pp. 254–261. MR MR2289128
- [113] M. F. Newman, *Addendum: “A computer aided study of a group defined by fourth powers”* (Bull. Austral. Math. Soc. **14** (1976), no. 2, 293–297), Bull. Austral. Math. Soc. **15** (1976), no. 3, 477–479. MR MR0435192 (55 #8153)
- [114] ———, *Some group presentations and enforcing the associative law*, Algebraic algorithms and error correcting codes (Grenoble, 1985), Lecture Notes in Comput. Sci., vol. 229, Springer, Berlin, 1986, pp. 228–237. MR MR864243 (88d:20038)
- [115] M. F. Newman, Werner Nickel, and Alice C. Niemeyer, *Descriptions of groups of prime-power order*, J. Symbolic Comput. **25** (1998), no. 5, 665–682. MR MR1617995 (99f:20054)
- [116] M. F. Newman and E. A. O’Brien, *A CAYLEY library for the groups of order dividing 128*, Group Theory (Singapore, 1987), de Gruyter, Berlin, 1989, pp. 437–442. MR MR981861 (90b:20002)
- [117] ———, *A computer-aided analysis of some finitely presented groups*, J. Austral. Math. Soc. Ser. A **53** (1992), no. 3, 369–376. MR MR1187855 (93k:20003)

- [118] ———, *Application of computers to questions like those of Burnside. II*, Internat. J. Algebra Comput. **6** (1996), no. 5, 593–605. MR MR1419133 (97k:20002)
- [119] ———, *Classifying 2-groups by coclass*, Trans. Amer. Math. Soc. **351** (1999), no. 1, 131–169. MR MR1458332 (99c:20020)
- [120] Alice C. Niemeyer, *A finite soluble quotient algorithm*, J. Symbolic Comput. **18** (1994), no. 6, 541–561. MR MR1334661 (96j:20001)
- [121] ———, *Computing finite soluble quotients*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 75–82. MR MR1344922 (96g:20023)
- [122] ———, *Constructive recognition of normalizers of small extra-special matrix groups*, Internat. J. Algebra Comput. **15** (2005), no. 2, 367–394. MR MR2142090
- [123] Alice C. Niemeyer and Cheryl E. Praeger, *A recognition algorithm for classical groups over finite fields*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 117–169. MR MR1625479 (99k:20002)
- [124] E. A. O’Brien, *The  $p$ -group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-6, 677–698, Computational group theory, Part 1. MR MR1075431 (91j:20050)
- [125] ———, *Isomorphism testing for  $p$ -groups*, J. Symbolic Comput. **17** (1994), no. 2, 131, 133–147. MR MR1283739 (95f:20040b)
- [126] ———, *Computing automorphism groups of  $p$ -groups*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 83–90. MR MR1344923 (96g:20024)
- [127] ———, *Towards effective algorithms for linear groups*, Finite Geometries, Groups, and Computation, Walter de Gruyter GmbH & Co. KG, Berlin, 2006, pp. 163–190. MR MR2258009
- [128] E. A. O’Brien and M. R. Vaughan-Lee, *The groups with order  $p^7$  for odd prime  $p$* , J. Algebra **292** (2005), no. 1, 243–258. MR MR2166803
- [129] Igor Pak, *The product replacement algorithm is polynomial*, 41st Annual Symposium on Foundations of Computer Science (Redondo Beach, CA, 2000), IEEE Comput. Soc. Press, Los Alamitos, CA, 2000, pp. 476–485. MR MR1931844



- [130] ———, *What do we know about the product replacement algorithm?*, Groups and Computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 301–347. MR MR1829489 (2002d:20107)
- [131] Andrea Previtali, *Irreducible constituents of monomial representations*, J. Symbolic Comput. **41** (2006), no. 12, 1345–1359. MR MR2271329
- [132] Birgit Reinert and Dirk Zeckzer, *Coset enumeration using prefix Gröbner bases: an experimental approach*, LMS J. Comput. Math. **4** (2001), 74–134 (electronic). MR MR1835854 (2002c:20051)
- [133] Eric Robinson and Gene Cooperman, *A parallel architecture for disk-based computing over the baby monster and other large finite simple groups*, ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 2006, pp. 298–305.
- [134] Eric Robinson, Jürgen Müller, and Gene Cooperman, *A disk-based parallel implementation for direct condensation of large permutation modules*, ISSAC 2007, ACM, New York, 2007, pp. 315–322. MR MR2402277
- [135] Colva M. Roney-Dougal, *Conjugacy of subgroups of the general linear group*, Experiment. Math. **13** (2004), no. 2, 151–163. MR MR2068889 (2005i:20051)
- [136] Colva M. Roney-Dougal and William R. Unger, *Computing the primitive permutation groups of degree less than 1000*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 243–260. MR MR2278931
- [137] Mohamed Sayed, *Coset enumeration of groups generated by symmetric sets of involutions*, Int. J. Math. Math. Sci. (2005), no. 23, 3739–3750. MR MR2203768 (2006j:20003)
- [138] ———, *Double-coset enumeration algorithm for symmetrically generated groups*, Int. J. Math. Math. Sci. (2005), no. 5, 699–715. MR MR2173686
- [139] ———, *Combinatorial method in the coset enumeration of symmetrically generated groups*, Int. J. Comput. Math. **85** (2008), no. 7, 993–1001. MR MR2428981 (2009f:20001)
- [140] Gerhard J. A. Schneider, *Computing with endomorphism rings of modular representations*, J. Symbolic Comput. **9** (1990), no. 5-6, 607–636, Computational group theory, Part 1. MR MR1075427 (92a:20015)

- [141] Ákos Seress, *An introduction to computational group theory*, Notices Amer. Math. Soc. **44** (1997), no. 6, 671–679. MR MR1452069 (98e:20002)
- [142] ———, *Nearly linear time algorithms for permutation groups: an interplay between theory and practice*, Acta Appl. Math. **52** (1998), no. 1-3, 183–207, Algebra and combinatorics: interactions and applications (Königstein, 1994). MR MR1649697 (2000e:20008)
- [143] ———, *A unified approach to computations with permutation and matrix groups*, International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zürich, 2006, pp. 245–258. MR MR2275596 (2008a:20006)
- [144] Charles C. Sims, *Computing with subgroups of automorphism groups of finite groups*, ISSAC '97: Proceedings of the 1997 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 1997, pp. 400–403.
- [145] Michael C. Slattery, *Computing character degrees in  $p$ -groups*, J. Symbolic Comput. **2** (1986), no. 1, 51–58. MR MR839136 (87e:20019)
- [146] ———, *Computing double cosets in soluble groups*, J. Symbolic Comput. **31** (2001), no. 1-2, 179–192. MR MR1806214 (2001k:20001)
- [147] Leonard H. Soicher, *Computing with graphs and groups*, Topics in algebraic graph theory (Lowell W. Beineke and Robin J. Wilson, eds.), Encyclopedia of Mathematics and its Applications, vol. 102, Cambridge University Press, Cambridge, 2004, pp. 250–266. MR MR2125091 (2005m:05002)
- [148] Bernd Souvignier, *Decomposing homogeneous modules of finite groups in characteristic zero*, J. Algebra **322** (2009), no. 3, 948–956.
- [149] P. Christopher Staecker, *Computing twisted conjugacy classes in free groups using nilpotent quotients*, 2007.
- [150] Polina Strogova, *Finding a finite group presentation using rewriting*, Symbolic Rewriting Techniques (Ascona, 1995), Progr. Comput. Sci. Appl. Logic, vol. 15, Birkhäuser, Basel, 1998, pp. 267–276. MR MR1624600 (99d:20046)
- [151] Gernot Stroth, *Algorithms in pure mathematics*, Computational discrete mathematics, Lecture Notes in Comput. Sci., vol. 2122, Springer, Berlin, 2001, pp. 148–158. MR MR1911587 (2003f:68151)

- [152] W. R. Unger, *Computing the character table of a finite group*, J. Symbolic Comput. **41** (2006), no. 8, 847–862. MR MR2246713 (2007b:20023)
- [153] ———, *Computing the soluble radical of a permutation group*, J. Algebra **300** (2006), no. 1, 305–315. MR MR2228650 (2007b:20007)
- [154] N. A. Vavilov, V. I. Mysovskikh, and Yu. G. Teterin, *Computational group theory in St. Petersburg*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **236** (1997), no. Vopr. Teor. Predst. Algebr i Grupp. 5, 42–49, 215–216. MR MR1754443 (2001a:20001)
- [155] Katsushi Waki, *Calculation of direct summands of FG-modules*, Sci. Rep. Hirosaki Univ. **44** (1997), no. 2, 193–200. MR MR1619001 (99c:16006)
- [156] Michael Weller, *Konstruktion der konjugiertenklassen von untergruppen mit kleinem index in p-gruppen*, Dissertation, Universität-Gesamthochschule-Essen, 1993.
- [157] Michael Weller, *Construction of classes of subgroups of small index in p-groups*, Arch. Math. (Basel) **68** (1997), no. 2, 89–99. MR MR1425498 (98c:20038)

# ***K*-Theory**

## **All Areas**

19Xxx

- [1] Werner Bley and Stephen M. J. Wilson, *Computations in relative algebraic  $K$ -groups*, LMS J. Comput. Math. **12** (2009), 166–194. MR 2564571 (2010k:16013)
- [2] R. R. Bruner and J. P. C. Greenlees, *The connective  $K$ -theory of finite groups*, Mem. Amer. Math. Soc. **165** (2003), no. 785, viii+127. MR MR1997161 (2004e:19003)
- [3] Cecilia Busuioc, *The Steinberg symbol and special values of  $L$ -functions*, Trans. Amer. Math. Soc. **360** (2008), no. 11, 5999–6015. MR MR2425699
- [4] Matthias Künzer, *Nonisomorphic Verdier octahedra on the same base*, J. Homotopy Relat. Struct. **4** (2009), no. 1, 7–38. MR MR2520985
- [5] Sebastian Pauli and Florence Soriano-Gafiuk, *The discrete logarithm in logarithmic  $l$ -class groups and its applications in  $K$ -theory*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 367–378. MR MR2138008 (2006a:11155)
- [6] Guyan Robertson, *Torsion in boundary coinvariants and  $K$ -theory for affine buildings*, *K*-Theory **33** (2005), no. 4, 347–369. MR MR2220525

# Linear Algebra

## Linear Algebra and Matrices

15-xx

- [1] Nigel Boston, *Spaces of constant rank matrices over  $\text{GF}(2)$* , *Electron. J. Linear Algebra* **20** (2010), 1–5. MR MR2596442
- [2] Paul-Olivier Dehayé, *Joint moments of derivatives of characteristic polynomials*, *Algebra Number Theory* **2** (2008), no. 1, 31–68. MR MR2377362 (2009a:15075)
- [3] Marjeta Kramar, *The structure of irreducible matrix groups with submultiplicative spectrum*, *Linear Multilinear Algebra* **53** (2005), no. 1, 13–25. MR MR2114139 (2005j:15018)
- [4] R. V. Kravchenko and B. V. Petrenko, *Some formulas for the minimal number of generators of the direct sum of matrix rings*, 2007.
- [5] Sefi Ladkani, *On the periodicity of Coxeter transformations and the non-negativity of their Euler forms*, *Linear Algebra Appl.* **428** (2008), no. 4, 742–753. MR MR2382086 (2009b:16037)
- [6] Zhongshan Li, Frank Hall, and Fuzhen Zhang, *Sign patterns of nonnegative normal matrices*, *Proceedings of the Fifth Conference of the International Linear Algebra Society (Atlanta, GA, 1995)*, vol. 254, 1997, pp. 335–354. MR MR1436685 (97m:15041)

# Computational Linear Algebra

- [1] Martin Albrecht, Gregory Bard, and William Hart, *Algorithm 898: Efficient multiplication of dense matrices over  $GF(2)$* , TOMS **37** (2010), no. 1.
- [2] Martin R. Albrecht and Clément Pernet, *Efficient decomposition of dense matrices over  $GF(2)$* , 2010, pp. 1–17.
- [3] Tomas J. Boothby and Robert W. Bradshaw, *Bitslicing and the method of four Russians over larger finite fields*, 2009, pp. 1–10.
- [4] Jean-Guillaume Dumas, Thierry Gautier, Pascal Giorgi, and Clément Pernet, *Dense linear algebra over finite fields: The FFLAS and FFPACK packages*, 2006.
- [5] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet, *FFPACK: finite field linear algebra package*, ISSAC '2004: Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2004, pp. 119–126. MR MR2126933
- [6] Jean-Guillaume Dumas, Pascal Giorgi, and Clément Pernet, *Dense linear algebra over word-size prime fields: The FFLAS and FFPACK packages*, ACM Trans. Math. Softw. **35** (2008), no. 3, 1–42.
- [7] Jean-Guillaume Dumas, Clément Pernet, and Zhendong Wan, *Efficient computation of the characteristic polynomial*, ISSAC'05: Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2005, pp. 140–147 (electronic). MR MR2280540
- [8] Jean-Guillaume Dumas and Anna Urbanska, *An introspective algorithm for the integer determinant*, 2006.
- [9] Wayne Eberly, Mark Giesbrecht, Pascal Giorgi, Arne Storjohann, and Gilles Villard, *Faster inversion and other black box matrix computations using efficient block projections*, ISSAC 2007, ACM, New York, 2007, pp. 143–150. MR MR2396196 (2009d:15008)
- [10] Cesar A. Garcia-Vazquez and Carlos A. Lopez-Andrade, *D-Heaps as hash tables for vectors over a finite ring*, 2009 WRI World Conference on Computer Science and

- Information Engineering, WRI World Congress on Computer Science and Information Engineering, vol. 3, IEEE, 2009, pp. 162–166.
- [11] Katharina Geißler and Nigel P. Smart, *Computing the  $M = UU^t$  integer matrix decomposition*, Cryptography and Coding, Lecture Notes in Comput. Sci., vol. 2898, Springer, Berlin, 2003, pp. 223–233. MR MR2090935 (2005e:94144)
- [12] George Havas, Derek F. Holt, and Sarah Rees, *Recognizing badly presented  $\mathbf{Z}$ -modules*, Linear Algebra Appl. **192** (1993), 137–163, Computational linear algebra in algebraic and related problems (Essen, 1992). MR MR1236741 (94i:20001)
- [13] George Havas, Bohdan S. Majewski, and Keith R. Matthews, *Extended GCD and Hermite normal form algorithms via lattice basis reduction*, Experiment. Math. **7** (1998), no. 2, 125–136. MR MR1677095 (2000k:11141a)
- [14] ———, *Addenda and errata: “Extended GCD and Hermite normal form algorithms via lattice basis reduction”*, Experiment. Math. **8** (1999), no. 2, 205. MR MR1700579 (2000k:11141b)
- [15] Gerold Jaeger, *Parallel algorithms for computing the Smith normal form of large matrices*, Recent Advances in Parallel Virtual Machine and Message Passing Interface, vol. 2840, Springer, Berlin/Heidelberg, 2003, pp. 170–179.
- [16] G. Jäger, *Reduction of Smith normal form transformation matrices*, Computing **74** (2005), no. 4, 377–388. MR MR2149345 (2006a:65068)
- [17] Frank Lübeck, *On the computation of elementary divisors of integer matrices*, J. Symbolic Comput. **33** (2002), no. 1, 57–65. MR MR1876312 (2002i:15002)
- [18] Max Neunhöffer and Cheryl E. Praeger, *Computing minimal polynomials of matrices*, LMS J. Comput. Math. **11** (2008), 252–279. MR MR2429999
- [19] Michael E. O’Sullivan, *Algebraic construction of sparse matrices with large girth*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 718–727. MR MR2236186
- [20] Clément Pernet and Arne Storjohann, *Faster algorithms for the characteristic polynomial*, ISSAC 2007, ACM, New York, 2007, pp. 307–314. MR MR2402276
- [21] Håvard Raddum and Igor Semaev, *Solving multiple right hand sides linear equations*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 147–160. MR MR2438447

- [22] Michael Schmid, Rainer Steinwandt, Jörn Müller-Quade, Martin Rötteler, and Thomas Beth, *Decomposing a matrix into circulant and diagonal factors*, Linear Algebra Appl. **306** (2000), no. 1-3, 131–143. MR MR1740437 (2000j:15027)
- [23] Igor Semaev, *Sparse boolean equations and circuit lattices*, 2009.
- [24] Allan Steel, *A new algorithm for the computation of canonical forms of matrices over fields*, J. Symbolic Comput. **24** (1997), no. 3-4, 409–432. MR MR1484489 (98m:65070)
- [25] Patrick Theobald, *Ein framework zur berechnung der hermite-normalform von grössen, dünnbesetzten, ganzzahligen matrizen*, PhD Thesis, Technischen Universität Darmstadt, 2000.
- [26] Gilles Villard, *Certification of the QR factor R and of lattice basis reducedness*, ISSAC 2007, ACM, New York, 2007, pp. 361–368. MR MR2402283



# Mathematical Education

## Computer-Assisted Learning

97Xxx

- [1] Nuh Aydin, *Enhancing undergraduate mathematics curriculum via coding theory and cryptography*, PRIMUS **19** (2009), no. 3, 296–309.
- [2] Nigel Boston, *A use of computers to teach group theory and introduce students to research*, J. Symbolic Comput. **23** (1997), no. 5–6, 453–458.
- [3] John Cannon and Catherine Playoust, *Using the Magma computer algebra system in abstract algebra courses*, J. Symbolic Comput. **23** (1997), no. 5–6, 459–484.
- [4] Erich Kaltofen, *Teaching computational abstract algebra*, J. Symbolic Comput. **23** (1997), no. 5–6, 503–515.
- [5] Gary J. Sherman, *Trying to do group theory with undergraduates and computers*, J. Symbolic Comput. **23** (1997), no. 5–6, 577–587.

# Number Theory

## Elementary Number Theory

11Axx except 11A41 and 11A51, 11Cxx

- [1] David H. Bailey and Jonathan M. Borwein, *Experimental mathematics: Examples, methods and implications*, Notices Amer. Math. Soc. **52** (2005), no. 5, 502–514. MR MR2140093
- [2] Wieb Bosma, *Some computational experiments in number theory*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 1–30. MR MR2278921
- [3] Richard P. Brent and Paul Zimmermann, *Ten new primitive binary trinomials*, Math. Comp. **78** (2009), no. 266, 1197–1199. MR MR2476580
- [4] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR MR1228206 (94i:11105)
- [5] ———, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000. MR MR1728313 (2000k:11144)
- [6] J. E. Cremona, *Unimodular integer circulants*, Math. Comp. **77** (2008), no. 263, 1639–1652. MR MR2398785
- [7] Vassil S. Dimitrov and Everett W. Howe, *Lower bounds on the lengths of double-base representations*.
- [8] Graham Everest and Valéry Mahé, *A generalization of Siegel’s theorem and Hall’s conjecture*, Experiment. Math. **18** (2009), no. 1, 1–9. MR MR2548983
- [9] Alina Ostafe and Igor E. Shparlinski, *Pseudorandomness and dynamics of Fermat quotients*, 2010.
- [10] Emmanuel Royer, *Evaluating convolution sums of the divisor function with quasimodular forms*, Int. J. Number Theory **3** (2007), no. 2, 231–261.
- [11] J. Sándor and B. Crstici, *Handbook of Number Theory II*, Kluwer Academic Publishers, Dordrecht, 2004. MR MR2119686 (2005k:11001)

# Primality and Factorisation

11A41, 11A51

- [1] Wieb Bosma, *Explicit primality criteria for  $h \cdot 2^k \pm 1$* , Math. Comp. **61** (1993), no. 203, 97–109. MR MR1197510 (94c:11005)
- [2] Richard P. Brent, Peter L. Montgomery, Herman J.J. te Riele, Henk Boender, Stephania Cavallar, Conrad Curry, Bruce Dodson, Jens Franke, Joseph Leherbauer, George Sassoan, and Robert Silverman, *Factorizations of cunningham numbers with bases 13 to 99: Millennium edition*, Report – Modelling, Analysis and Simulation, vol. 7, Centrum voor Wiskunde en Informatica, Amsterdam, 2001, pp. i–viii, pp. 1–19.
- [3] Graham Everest, Patrick Ingram, and Shaun Stevens, *Primitive divisors on twists of Fermat’s cubic*, LMS J. Comput. Math. **12** (2009), 54–81. MR MR2486632
- [4] Stephen McMath, *Parallel integer factorization using quadratic forms*, 2005.
- [5] F. Morain, *Primality proving using elliptic curves: An update*, Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 111–127. MR MR1726064 (2000i:11190)
- [6] Paul Zimmermann and Bruce Dodson, *20 years of ECM*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 525–542. MR MR2282947

# Sequences and Sets

11Bxx

- [1] S. Akhtari, A. Togbé, and P. G. Walsh, *On the equation  $aX^4 - bY^2 = 2$* , Acta Arith. **131** (2008), no. 2, 145–169. MR MR2388048
- [2] Huseyin Aydin, Ramazan Dikici, and Geoff C. Smith, *Wall and Vinson revisited*, Applications of Fibonacci Numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 61–68. MR MR1271347 (95f:11009)
- [3] Alexander Berkovich and William C. Jagy, *Ternary quadratic forms, modular equations and certain positivity conjectures*, The Legacy of Alladi Ramakrishnan in the Mathematical Sciences (Krishnaswami Alladi, John R. Klauder, and Calyampudi R. Rao, eds.), Springer, New York, 2009, pp. 211–241.
- [4] A. Bremner and N. Tzanakis, *Lucas sequences whose 12th or 9th term is a square*, J. Number Theory **107** (2004), no. 2, 215–227. MR MR2072385 (2005i:11019)
- [5] ———, *Lucas sequences whose 8th term is a square*, 2004.
- [6] ———, *On squares in Lucas sequences*, J. Number Theory **124** (2007), no. 2, 511–520. MR MR2321377
- [7] Florian Breuer, Ernest Lötter, and Brink van der Merwe, *Ducci-sequences and cyclotomic polynomials*, Finite Fields Appl. **13** (2007), no. 2, 293–304. MR MR2307129 (2008a:11017)
- [8] N. Bruin, K. Györy, L. Hajdu, and Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. (N.S.) **17** (2006), no. 4, 539–555. MR MR2320112 (2008e:11036)
- [9] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *On Fibonacci numbers with few prime divisors*, Proc. Japan Acad. Ser. A Math. Sci. **81** (2005), no. 2, 17–20. MR MR2126070 (2005k:11020)
- [10] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *Sur les nombres de Fibonacci de la forme  $q^k y^p$* , C. R. Math. Acad. Sci. Paris **339** (2004), no. 5, 327–330. MR MR2092057 (2005g:11019)

- [11] Enrique Gonzalez-Jimenez and Xavier Xarles, *Five squares in arithmetic progression over quadratic fields*, 2009.
- [12] Everett W. Howe, *Higher-order Carmichael numbers*, *Math. Comp.* **69** (2000), no. 232, 1711–1719. MR MR1709151 (2001a:11012)
- [13] Benjamin Kane, *Representing sets with sums of triangular numbers*, *Int. Math. Res. Not. IMRN* (2009), no. 17, 3264–3285. MR MR2534998
- [14] Tünde Kovács, *Combinatorial numbers in binary recurrences*, *Period. Math. Hungar.* **58** (2009), no. 1, 83–98. MR MR2487248 (2010a:11024)
- [15] J. McLaughlin, *Small prime powers in the Fibonacci sequence*, 2002.
- [16] A. Stoimenow, *Generating functions, Fibonacci numbers and rational knots*, *J. Algebra* **310** (2007), no. 2, 491–525. MR MR2308169 (2008a:05018)

# Diophantine Equations

11Dxx

- [1] Fadwa S. Abu Muriefah, Florian Luca, and Alain Togbé, *On the Diophantine equation  $x^2 + 5^a 13^b = y^n$* , *Glasg. Math. J.* **50** (2008), no. 1, 175–181. MR MR2381741 (2008m:11071)
- [2] S. Akhtari, A. Togbé, and P. G. Walsh, *On the equation  $aX^4 - bY^2 = 2$* , *Acta Arith.* **131** (2008), no. 2, 145–169. MR MR2388048
- [3] Shabnam Akhtari, *The diophantine equation  $ax^4 - by^2 = 1$* , 2009.
- [4] ———, *The method of Thue-Siegel for binary quartic forms*, 2009.
- [5] M. A. Bennett, N. Bruin, K. Győry, and L. Hajdu, *Powers from products of consecutive terms in arithmetic progression*, *Proc. London Math. Soc. (3)* **92** (2006), no. 2, 273–306. MR MR2205718 (2006k:11046)
- [6] Michael A. Bennett, *The Diophantine equation  $(x^k - 1)(y^k - 1) = (z^k - 1)^t$* , *Indag. Math. (N.S.)* **18** (2007), no. 4, 507–525. MR MR2424310 (2009b:11058)
- [7] Michael A. Bennett, Kálmán Győry, and Ákos Pintér, *On the Diophantine equation  $1^k + 2^k + \dots + x^k = y^n$* , *Compos. Math.* **140** (2004), no. 6, 1417–1431. MR MR2098395 (2005g:11042)
- [8] A. Bérczes, A. Pethő, and V. Ziegler, *Parameterized norm form equations with arithmetic progressions*, *J. Symbolic Comput.* **41** (2006), no. 7, 790–810. MR MR2232201 (2007c:11040)
- [9] Attila Bérczes and Attila Pethő, *Computational experiences on norm form equations with solutions forming arithmetic progressions*, *Glas. Mat. Ser. III* **41(61)** (2006), no. 1, 1–8. MR MR2242387 (2007g:11040)
- [10] A. Bremner and Jean-Joël Delorme., *On equal sums of ninth powers*, *Math. Comp* **79** (2009), 603–612.
- [11] A. Bremner and N. Tzanakis, *Lucas sequences whose 8th term is a square*, 2004.
- [12] ———, *On squares in Lucas sequences*, *J. Number Theory* **124** (2007), no. 2, 511–520. MR MR2321377

- [13] Andrew Bremner, *On the equation  $Y^2 = X^5 + k$* , Experiment. Math. **17** (2008), no. 3, 371–374. MR MR2455707
- [14] ———, *A problem of Ozanam*, Proc. Edinb. Math. Soc. (2) **52** (2009), no. 1, 37–44. MR MR2475879
- [15] Andrew Bremner and Nikos Tzanakis, *On the equation  $y^2 = x^6 + k$* , Annales des Sciences Mathématiques du Québec **To appear** (2010).
- [16] David Brown, *Primitive integral solutions to  $x^2 + y^3 = z^{10}$* , 2009.
- [17] N. Bruin, K. Győry, L. Hajdu, and Sz. Tengely, *Arithmetic progressions consisting of unlike powers*, Indag. Math. (N.S.) **17** (2006), no. 4, 539–555. MR MR2320112 (2008e:11036)
- [18] Nils Bruin, *The primitive solutions to  $x^3 + y^9 = z^2$* , J. Number Theory **111** (2005), no. 1, 179–189. MR MR2124048
- [19] ———, *Some ternary Diophantine equations of signature  $(n, n, 2)$* , Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 63–91. MR MR2278923
- [20] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884
- [21] Nils Bruin and Michael Stoll, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.
- [22] Ralph H. Buchholz, *Triangles with three rational medians*, J. Number Theory **97** (2002), no. 1, 113–131. MR MR1939139 (2003h:11034)
- [23] Ralph H. Buchholz and James A. MacDougall, *Cyclic polygons with rational sides and area*, J. Number Theory **128** (2008), no. 1, 17–48. MR MR2382768 (2008m:11061)
- [24] Yann Bugeaud, Florian Luca, Maurice Mignotte, and Samir Siksek, *On perfect powers in Lucas sequences*, Int. J. Number Theory **1** (2005), no. 3, 309–332. MR MR2175095
- [25] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *Classical and modular approaches to exponential Diophantine equations I: Fibonacci and Lucas perfect powers*, Ann. of Math. (2) **163** (2006), no. 3, 969–1018. MR MR2215137 (2007f:11031)

- [26] ———, *Classical and modular approaches to exponential Diophantine equations II: The Lebesgue-Nagell equation*, Compos. Math. **142** (2006), no. 1, 31–62. MR MR2196761 (2007f:11032)
- [27] ———, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canad. J. Math. **60** (2008), no. 3, 491–519. MR MR2414954 (2009b:11059)
- [28] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885. MR MR2457355
- [29] I. N. Cangül, M. Demirci, G. Soydan, and N. Tzanakis., *On the diophantine equation  $x^2 + 5^a \cdot 11^b = y^n$* , 2011, p. 21 pages.
- [30] Imin Chen, *A Diophantine equation associated to  $X_0(5)$* , LMS J. Comput. Math. **8** (2005), 116–121 (electronic). MR MR2153792 (2006b:11052)
- [31] ———, *On the equation  $s^2 + y^{2p} = \alpha^3$* , Math. Comp. **77** (2008), no. 262, 1223–1227. MR MR2373199
- [32] Imin Chen and Samir Siksek, *Perfect powers expressible as sums of two cubes*, J. Algebra **322** (2009), no. 3, 638–656. MR MR2531215
- [33] C. Chisholm and J. A. MacDougall, *Rational and Heron tetrahedra*, J. Number Theory **121** (2006), no. 1, 153–185. MR MR2268761 (2007h:11040)
- [34] ———, *Rational tetrahedra with edges in geometric progression*, J. Number Theory **128** (2008), no. 2, 251–262. MR MR2380320
- [35] Mihai Cipu, *Gröbner bases and Diophantine analysis*, J. Symbolic Comput. **43** (2008), no. 10, 681–687. MR MR2426566
- [36] Mihai Cipu, Florian Luca, and Maurice Mignotte, *Solutions of the Diophantine equation  $x^y + y^z + z^x = n!$* , Glasg. Math. J. **50** (2008), no. 2, 217–232. MR MR2417617
- [37] Henri Cohen, *Number theory: Volume I: Tools and diophantine equations*, Springer, Berlin, 2007.
- [38] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR MR2212121 (2006m:11042)



- [39] Robert S. Coulter, Marie Henderson, and Felix Lazebnik, *On certain combinatorial Diophantine equations and their connection to Pythagorean numbers*, Acta Arith. **122** (2006), no. 4, 395–406. MR MR2234423 (2007a:11036)
- [40] R. de la Bret'che and T.D. Browning, *Manin's conjecture for quartic del Pezzo surfaces with a conic fibration*, 2008.
- [41] Luis V. Dieulefait, *Solving Diophantine equations  $x^4 + y^4 = qz^p$* , Acta Arith. **117** (2005), no. 3, 207–211. MR MR2139003 (2005k:11059)
- [42] Shanshan Ding, *Smallest irreducible of the form  $x^2 - dy^2$* , 2007.
- [43] Konstantinos Draziotis and Dimitrios Poulakis, *Practical solution of the Diophantine equation  $y^2 = x(x + 2^ap^b)(x - 2^ap^b)$* , Math. Comp. **75** (2006), no. 255, 1585–1593 (electronic). MR MR2219047 (2007b:11192)
- [44] ———, *Corrigendum to “Solving the Diophantine equation  $y^2 = x(x^2 - n^2)$ ” [J. Number Theory 129 (1) (2009) 102–121] [mr2468473]*, J. Number Theory **129** (2009), no. 3, 739–740. MR MR2488600 (2010c:11040)
- [45] ———, *Solving the Diophantine equation  $y^2 = x(x^2 - n^2)$* , J. Number Theory **129** (2009), no. 1, 102–121. MR MR2468473 (2009j:11047)
- [46] Konstantinos A. Draziotis, *Integer points on the curve  $Y^2 = X^3 \pm p^kX$* , Math. Comp. **75** (2006), no. 255, 1493–1505 (electronic). MR MR2219040 (2007a:11034)
- [47] Edray Goins, Florian Luca, and Alain Togbé, *On the Diophantine equation  $x^2 + 2^\alpha 5^\beta 13^\gamma = y^n$* , Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 430–442. MR MR2467863
- [48] Enrique Gonzalez-Jimenez and Xavier Xarles, *Five squares in arithmetic progression over quadratic fields*, 2009.
- [49] K. Györy, L. Hajdu, and Á. Pintér, *Perfect powers from products of consecutive terms in arithmetic progression*, Compos. Math. **145** (2009), no. 4, 845–864. MR MR2521247 (2010d:11037)
- [50] K. Györy and Á. Pintér, *Almost perfect powers in products of consecutive integers*, Monatsh. Math. **145** (2005), no. 1, 19–33. MR MR2134477 (2006a:11040)

- [51] ———, *Correction to the paper: “Almost perfect powers in products of consecutive integers”*, Monatsh. Math. **146** (2005), no. 4, 341. MR MR2191733 (2006i:11036)
- [52] ———, *On the resolution of equations  $Ax^n - By^n = C$  in integers  $x, y$  and  $n \geq 3$ . I*, Publ. Math. Debrecen **70** (2007), no. 3-4, 483–501. MR MR2310662 (2008g:11053)
- [53] Lajos Hajdu and Szabolcs Tengely, *Arithmetic progressions of squares, cubes and  $n$ -th powers*, Funct. Approx. Comment. Math. **41** (2009), no. 2, 129–138. MR MR2590329
- [54] Lajos Hajdu, Szabolcs Tengely, and Robert Tijdeman, *Cubes in products of terms in arithmetic progression*, Publ. Math. Debrecen **74** (2009), no. 1-2, 215–232. MR MR2490432 (2009j:11050)
- [55] Robin Hartshorne and Ronald van Luijk, *Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on K3 surfaces*, Math. Intelligencer **30** (2008), no. 4, 4–10. MR MR2501390
- [56] Bo He and Alain Togbé, *On the number of solutions of Goormaghtigh equation for given  $x$  and  $y$* , Indag. Math. (N.S.) **19** (2008), no. 1, 65–72. MR MR2466394 (2009i:11042)
- [57] E. Herrmann, I. Járási, and A. Pethő, *Note on: “The Diophantine equation  $x^n = Dy^2 + 1$ ” by J. H. E. Cohn*, Acta Arith. **113** (2004), no. 1, 69–76. MR MR2046969 (2004m:11046)
- [58] E. Herrmann, F. Luca, and P. G. Walsh, *A note on the Ramanujan-Nagell equation*, Publ. Math. Debrecen **64** (2004), no. 1-2, 21–30. MR MR2035886 (2004k:11033)
- [59] Emanuel Herrmann and Attila Pethő,  *$S$ -integral points on elliptic curves. Notes on a paper of B. M. M. de Weger*, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 443–451. MR MR1881378 (2003a:11024)
- [60] Akinari Hoshi, *On the simplest quartic fields and related Thue equations*, 2010.
- [61] Stephen P. Humphries and Kenneth W. Johnson, *Fusions of character tables and Schur rings of abelian groups*, Comm. Algebra **36** (2008), no. 4, 1437–1460. MR MR2406596 (2009b:20008)
- [62] Benjamin Kane, *Representing sets with sums of triangular numbers*, Int. Math. Res. Not. IMRN (2009), no. 17, 3264–3285. MR MR2534998

- [63] Tünde Kovács, *Combinatorial Diophantine equations—the genus 1 case*, Publ. Math. Debrecen **72** (2008), no. 1-2, 243–255. MR MR2376872 (2008m:11065)
- [64] Shanta Laishram, T. N. Shorey, and Szabolcs Tengely, *Squares in products in arithmetic progression with at most one term omitted and common difference a prime power*, Acta Arith. **135** (2008), no. 2, 143–158. MR MR2453529
- [65] A. Laradji, M. Mignotte, and N. Tzanakis, *On  $px^2 + q^{2n} = y^p$  and related Diophantine equations*, 2010.
- [66] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Coleman-Chabauty*, 2000.
- [67] F. Luca, P. Stanica, and A. Togbé, *On a Diophantine equation of Stroeker*, Bull. Belg. Math. Soc. Simon Stevin (2008), 10.
- [68] Florian Luca and Alain Togbé, *On the Diophantine equation  $x^2 + 2^\alpha 13^\beta = y^n$* , Colloq. Math. **116** (2009), no. 1, 139–146. MR MR2504836
- [69] Florian Luca and Peter Gareth Walsh, *On a sequence of integers arising from simultaneous Pell equations*, Funct. Approx. Comment. Math. **38** (2008), no. , part 2, 221–226. MR MR2492857 (2010b:11036)
- [70] F. S. Abu Muriefah, F. Luca, S. Siksek, and S. Tengely, *On the Diophantine equation  $x^2 + c = 2y^n$* , Int. J. Number Theory (2008).
- [71] Á. Pintér, *On a class of Diophantine equations related to the numbers of cells in hyperplane arrangements*, J. Number Theory **129** (2009), no. 7, 1664–1668. MR MR2524187
- [72] Ákos Pintér, *On the power values of power sums*, J. Number Theory **125** (2007), no. 2, 412–423. MR MR2332596 (2008g:11052)
- [73] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of  $X(7)$  and primitive solutions to  $x^2 + y^3 = z^7$* , Duke Math. J. **137** (2007), no. 1, 103–158. MR MR2309145
- [74] Diana Savin, *About certain prime numbers*, 2009, p. 9.
- [75] Samir Siksek, *The modular approach to diophantine equations*, Number Theory (Henri Cohen, ed.), Graduate Texts in Mathematics, vol. 240, Springer, New York, 2007, pp. 495–527.

- [76] Samir Siksek and John E. Cremona, *On the Diophantine equation  $x^2 + 7 = y^m$* , Acta Arith. **109** (2003), no. 2, 143–149. MR MR1980642 (2004c:11109)
- [77] Samir Siksek and Michael Stoll, *On a problem of Hajdu and Tengely*, 2009.
- [78] N. P. Smart, *Thue and Thue-Mahler equations over rings of integers*, J. London Math. Soc. (2) **56** (1997), no. 3, 455–462. MR MR1610439 (99d:11031)
- [79] Nigel P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998. MR MR1689189 (2000c:11208)
- [80] Sz. Tengely, *Note on the paper: “An extension of a theorem of Euler” by N. Hirata-Kohno, S. Laishram, T. N. Shorey and R. Tijdeman*, Acta Arith. **134** (2008), no. 4, 329–335. MR MR2449156 (2009h:11050)
- [81] Szabolcs Tengely, *On the Diophantine equation  $x^2 + a^2 = 2y^p$* , Indag. Math. (N.S.) **15** (2004), no. 2, 291–304. MR MR2071862 (2005f:11045)
- [82] ———, *Effective methods for Diophantine equations*, Ph.D. thesis, Leiden University, 2005, p. 85.
- [83] ———, *Triangles with two integral sides*, Ann. Math. Inform. **34** (2007), 89–95. MR MR2385428 (2009a:11070)
- [84] P. G. Walsh, *On a very particular class of Ramanujan-Nagell type equations*, Far East J. Math. Sci. (FJMS) **24** (2007), no. 1, 55–58. MR MR2281854 (2007k:11213)
- [85] Huilin Zhu and Jianhua Chen, *Integral points on a class of elliptic curve*, Wuhan Univ. J. Nat. Sci. **11** (2006), no. 3, 477–480. MR MR2258847 (2007d:11064)

# Forms and Linear Algebraic Groups

11Exx

- [1] Kanat Abdukhalikov and Rudolf Scharlau, *Unimodular lattices in dimensions 14 and 15 over the Eisenstein integers*, Math. Comp. **78** (2009), no. 265, 387–403. MR MR2448712
- [2] Alexander Berkovich and William C. Jagy, *Ternary quadratic forms, modular equations and certain positivity conjectures*, The Legacy of Alladi Ramakrishnan in the Mathematical Sciences (Krishnaswami Alladi, John R. Klauder, and Calyampudi R. Rao, eds.), Springer, New York, 2009, pp. 211–241.
- [3] Manjul Bhargava, *Higher composition laws I: A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2) **159** (2004), no. 1, 217–250. MR MR2051392 (2005f:11062a)
- [4] Donald I. Cartwright and Tim Steger, *Application of the Bruhat–Tits tree of  $SU_3(h)$  to some  $A_2$  groups*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 3, 329–344. MR MR1623286 (99i:11026)
- [5] Carlos Castaño-Bernard, *Further properties of a function of Ogg and Ligozat*, Ramanujan J. **17** (2008), no. 1, 107–121. MR MR2439528
- [6] Darrin Doud, *Supersingular Galois representations and a generalization of a conjecture of Serre*, Experiment. Math. **16** (2007), no. 1, 119–128. MR MR2312982 (2007m:11076)
- [7] Paul E. Gunnells and Dan Yasaki, *Perfect forms over totally real number fields*, 2009.
- [8] Jonathan Hanke, *Local densities and explicit bounds for representability by a quadratic form*, Duke Math. J. **124** (2004), no. 2, 351–388. MR MR2079252 (2005m:11060)
- [9] Boris Hemkemeier, *Algorithmische Konstruktionen von Gittern*, 2004.
- [10] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.
- [11] Piotr Maciak, *Primes of the form  $x^2 + n * y^2$  in function fields*, 2009.

- [12] Jeremy Rouse, *Zagier duality for the exponents of Borcherds products for Hilbert modular forms*, J. London Math. Soc. (2) **73** (2006), no. 2, 339–354. MR MR2225490 (2006m:11059)
- [13] John Voight, *Quadratic Forms and Quaternion Algebras: Algorithms and Arithmetic*, Ph.D. thesis, Berkeley, 2005, p. 98.
- [14] John Voight, *Quadratic forms that represent almost the same primes*, Math. Comp. **76** (2007), no. 259, 1589–1617 (electronic). MR MR2299790 (2007m:11055)
- [15] Tonghai Yang, *Local densities of 2-adic quadratic forms*, J. Number Theory **108** (2004), no. 2, 287–345. MR MR2098640 (2005i:11048)
- [16] Dan Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), no. 11, 4132–4142. MR MR2556143
- [17] Dan Yasaki, *Hyperbolic tessellations associated to Bianchi groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 385–396.

# Discontinuous Groups and Automorphic Forms

11Fxx

- [1] Scott Ahlgren, *On the irreducibility of Hecke polynomials*, Math. Comp. **77** (2008), no. 263, 1725–1731. MR MR2398790
- [2] Scott Ahlgren and Ken Ono, *Arithmetic of singular moduli and class polynomials*, Compos. Math. **141** (2005), no. 2, 293–312. MR MR2134268 (2006a:11058)
- [3] A. O. L. Atkin, Wen-Ching Winnie Li, and Ling Long, *On Atkin and Swinnerton-Dyer congruence relations (II)*, Math. Ann. **340** (2008), no. 2, 335–358. MR MR2368983 (2009a:11102)
- [4] Tobias Berger, *An Eisenstein ideal for imaginary quadratic fields and the Bloch-Kato conjecture for Hecke characters*, 2007.
- [5] Tobias Berger and Krzysztof Klosin, *A deformation problem for Galois representations over imaginary quadratic fields*, J. Inst. Math. Jussieu **To appear** (2009), 19.
- [6] Alexander Berkovich and William C. Jagy, *Ternary quadratic forms, modular equations and certain positivity conjectures*, The Legacy of Alladi Ramakrishnan in the Mathematical Sciences (Krishnaswami Alladi, John R. Klauder, and Calyampudi R. Rao, eds.), Springer, New York, 2009, pp. 211–241.
- [7] Siegfried Boecherer and Gabriele Nebe, *On theta series attached to maximal lattices and their adjoints*, 2009.
- [8] Johan Bosman, *On the computation of Galois representations associated to level one modular forms*, 2007.
- [9] Jim Brown, *Saito-Kurokawa lifts and applications to the Bloch-Kato conjecture*, Compos. Math. **143** (2007), no. 2, 290–322. MR MR2309988
- [10] Jan Hendrik Bruinier and Tonghai Yang, *CM-values of Hilbert modular functions*, Invent. Math. **163** (2006), no. 2, 229–288.
- [11] Yann Bugeaud, Maurice Mignotte, and Samir Siksek, *A multi-Frey approach to some multi-parameter families of Diophantine equations*, Canad. J. Math. **60** (2008), no. 3, 491–519. MR MR2414954 (2009b:11059)

- [12] Cecilia Busuioc, *The Steinberg symbol and special values of L-functions*, Trans. Amer. Math. Soc. **360** (2008), no. 11, 5999–6015. MR MR2425699
- [13] Kevin Buzzard, *Questions about slopes of modular forms*, Astérisque (2005), no. 298, 1–15, Automorphic forms. I. MR MR2141701 (2005m:11082)
- [14] Kevin Buzzard and Frank Calegari, *A counterexample to the Gouvêa-Mazur conjecture*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 10, 751–753. MR MR2059481 (2005g:11070)
- [15] Kevin Buzzard and William A. Stein, *A mod five approach to modularity of icosahedral Galois representations*, Pacific J. Math. **203** (2002), no. 2, 265–282. MR MR1897901 (2003c:11052)
- [16] Bryden Cais, *Serre’s conjectures*, 2005.
- [17] Frank Calegari and Nathan M. Dunfield, *Automorphic forms and rational homology 3-spheres*, Geom. Topol. **10** (2006), 295–329 (electronic). MR MR2224458 (2007h:57013)
- [18] Frank Calegari and William A. Stein, *Conjectures about discriminants of Hecke algebras of prime level*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 140–152. MR MR2137350
- [19] Imin Chen, Ian Kiming, and Jonas B. Rasmussen, *On congruences mod  $p^m$  between eigenforms and their attached Galois representations*, J. Number Theory **130** (2010), no. 3, 608–619. MR MR2584844
- [20] C. J. Cummins, *Congruence subgroups of groups commensurable with  $PSL(2, Z)$  of genus 0 and 1*, Experiment. Math. **13** (2004), no. 3, 361–382. MR MR2103333 (2005i:11058)
- [21] C.J. Cummins, *On conjugacy classes of congruence subgroups of  $PSL(2, R)$* , LMS J. Comput. Math. **12** (2009), 264–274. MR 2570927
- [22] Henri Darmon and Robert Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. **153** (2006), 319–354. MR MR2254648
- [23] Lassina Dembélé, *Explicit computations of Hilbert modular forms on  $\mathbf{Q}(\sqrt{5})$* , Experiment. Math. **14** (2005), no. 4, 457–466. MR MR2193808 (2006h:11050)



- [24] ———, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, *Math. Comp.* **76** (2007), no. 258, 1039–1057 (electronic). MR MR2291849
- [25] Lassina Dembélé, *On the computation of algebraic modular forms on compact inner forms of  $GSp_4$* , 2009.
- [26] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, *Algorithmic number theory, Lecture Notes in Comput. Sci.*, vol. 5011, Springer, Berlin, 2008, pp. 371–386. MR MR2467859 (2010d:11149)
- [27] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, 2009.
- [28] Tobias Dern and Aloys Krieg, *Graded rings of Hermitian modular forms of degree 2*, *Manuscripta Math.* **110** (2003), no. 2, 251–272. MR MR1962537 (2004b:11059)
- [29] ———, *The graded ring of Hermitian modular forms of degree 2 over  $Q(\sqrt{-2})$* , *J. Number Theory* **107** (2004), no. 2, 241–265. MR MR2072387 (2005d:11069)
- [30] Michael Dewar and Olav K. Richter, *Ramanujan congruences for Siegel modular forms*, arXiv:0910.0787v1 (2009).
- [31] Meghan DeWitt and Darrin Doud, *Finding Galois representations corresponding to certain Hecke eigenclasses*, *Int. J. Number Theory* **5** (2009), no. 1, 1–11. MR MR2499017 (2009k:11091)
- [32] Luis Dieulefait, E. Gonzalez-Jimenez, and J. Jimenez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, arXiv:0909.1661v1 (2009).
- [33] Luis Dieulefait and Xavier Taixes i Ventosa, *Congruences between modular forms and lowering the level mod  $l^n$* , *Journal de Theorie des Nombres de Bordeaux* **31** (2009), no. 1, 109–118.
- [34] Darrin Doud, *Three-dimensional Galois representations with conjectural connections to arithmetic cohomology*, *Number Theory for the Millennium I (Urbana, IL, 2000)*, A K Peters, Natick, MA, 2002, pp. 365–375. MR MR1956235 (2003k:11089)
- [35] ———, *Distinguishing contragredient Galois representations in characteristic two*, *Rocky Mountain J. Math.* **38** (2008), no. 3, 835–848. MR MR2426523

- [36] Darrin Doud and Brian Hansen, *Explicit Frobenius calculations supporting a generalization of a conjecture of Serre*, JP J. Algebra Number Theory Appl. **6** (2006), no. 2, 381–398. MR MR2283945
- [37] Neil Dummigan, William Stein, and Mark Watkins, *Constructing elements in Shafarevich-Tate groups of modular motives*, Number Theory and Algebraic Geometry, London Math. Soc. Lecture Note Ser., vol. 303, Cambridge Univ. Press, Cambridge, 2003, pp. 91–118. MR MR2053457 (2005g:11071)
- [38] Bas Edixhoven, *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one*, J. Inst. Math. Jussieu **5** (2006), no. 1, 1–34, With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese. MR MR2195943 (2007f:11046)
- [39] Liqun Fang, J. William Hoffman, Benjamin Linowitz, Andrew Rupinski, and Helena Verrill, *Modular forms on noncongruence subgroups and Atkin-Swinnerton-Dyer relations*, Experiment. Math. **19** (2010), no. 1, 1–27.
- [40] Julio Fernández, Josep González, and Joan-C. Lario, *Plane quartic twists of  $X(5, 3)$* , Canad. Math. Bull. **50** (2007), no. 2, 196–205. MR MR2317442 (2008b:11067)
- [41] Sharon M. Frechette, *A classical characterization of newforms with equivalent eigenforms in  $S_{k+1/2}(4N, \chi)$* , J. London Math. Soc. (2) **68** (2003), no. 3, 563–578. MR MR2009437 (2004h:11040)
- [42] E. Freitag and R. Salvati Manni, *Some Siegel threefolds with a Calabi-Yau model II*, 2010.
- [43] Eberhard Freitag and Manabu Oura, *A theta relation in genus 4*, Nagoya Math. J. **161** (2001), 69–83. MR MR1820213 (2002m:11035)
- [44] Edray Goins, *On the modularity of wildly ramified Galois representations*, 2004.
- [45] Enrique Gonzalez-Jimenez and Xavier Guitart, *On the modularity level of modular abelian varieties over number fields*, J. Number Theory **130** (2010), no. 7, 1560–1570.
- [46] Matthew Greenberg and John Voight, *Computing systems of Hecke eigenvalues associated to Hilbert modular forms*, Math. Comp. **To appear** (2011).
- [47] Xavier Guitart and Jordi Quer, *Modular abelian varieties over number fields*, 2009.

- [48] P. E. Gunnells, F. Hajir, and D. Yasaki, *Modular forms and elliptic curves over the field of fifth roots of unity*, 2010.
- [49] Jerome W. Hoffman, Ling Long, and Helena Verrill, *On  $l$ -adic representations for a space of noncongruence cuspforms*, 2010.
- [50] Xavier Taixes i Ventosa and Gabor Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, arXiv:0909.2724v2 (2009).
- [51] Samar Jaafar and Kamal Khuri-Makdisi, *On the maps from  $X(4p)$  to  $X(4)$* , 2007.
- [52] Rafe Jones and Jeremy Rouse, *Iterated endomorphisms of abelian algebraic groups*, Proc. London Math. Soc. **100** (2010), 763–794.
- [53] Hidenori Katsurada, *Exact standard zeta values of Siegel modular forms*, Experiment. Math. **19** (2010), no. 1, 65–77.
- [54] L. J. P. Kilford, *Slopes of overconvergent modular forms*, PhD Thesis, Imperial College, University of London, 2002.
- [55] L. J. P. Kilford, *Generating spaces of modular forms with  $\eta$ -quotients*, JP J. Algebra Number Theory Appl. **8** (2007), no. 2, 213–226. MR MR2406859 (2009b:11075)
- [56] ———, *Modular forms*, Imperial College Press, London, 2008, A classical and computational introduction. MR MR2441106 (2009m:11001)
- [57] ———, *On mod  $p$  modular representations which are defined over  $\mathbb{F}_p$* , Glas. Mat. Ser. III **43(63)** (2008), no. 1, 1–6. MR MR2426658 (2009h:11070)
- [58] ———, *On the slopes of the  $U_5$  operator acting on overconvergent modular forms*, J. Théor. Nombres Bordeaux **20** (2008), no. 1, 165–182. MR MR2434162 (2009f:11045)
- [59] L. J. P. Kilford, *Experimental finding of modular forms for noncongruence subgroups*, 2009.
- [60] L. J. P. Kilford, *On the  $U_p$  operator acting on  $p$ -adic overconvergent modular forms when  $X_0(p)$  has genus 1*, J. Number Theory **130** (2010), no. 3, 586–594. MR MR2584842
- [61] L. J. P. Kilford and Gabor Wiese, *On the failure of the Gorenstein property for Hecke algebras of prime weight*, Experiment. Math. **17** (2008), no. 1, 37–52. MR 2410114 (2009c:11075)

- [62] L. J. P. Kilford and Gabor Wiese, *On mod  $p$  representations which are defined over  $F_p$ :  $I_i$* , Glasgow Math. J. **52** (2010), 391–400.
- [63] Ian Kiming, Matthias Schuett, and Helena Verrill, *Lifts of projective congruence groups*, J. London Math. Soc **To appear** (2010).
- [64] Ingo Herbert Klöcker, *Modular forms for the orthogonal group  $O(2, 5)$* , Ph.D. thesis, 2005, p. 142.
- [65] Aristides Kontogeorgis and Yifan Yang, *Automorphisms of hyperelliptic modular curves  $X_0(n)$  in positive characteristic*, LMS J. Comput. Math. **13** (2010), 144–163.
- [66] A. Krieg, *The graded ring of quaternionic modular forms of degree 2*, Math. Z. **251** (2005), no. 4, 929–942. MR MR2190150
- [67] Dominic Lanphier, *Combinatorics of Maass-Shimura operators*, J. Number Theory **128** (2008), no. 8, 2467–2487. MR MR2394832
- [68] Joan-C. Lario and René Schoof, *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311, With an appendix by Amod Agashe and William Stein. MR MR1959271 (2004b:11072)
- [69] Mark Lingham, *Modular Forms and Elliptic Curves over Imaginary Quartic Fields*, PhD Thesis, University of Nottingham, 2005.
- [70] David Loeffler, *Explicit calculations of automorphic forms for definite unitary groups*, LMS J. Comput. Math. **11** (2008), 326–342. MR MR2452552 (2009i:11062)
- [71] David Loeffler and Jared Weinstein, *On the computation of local components of a newform*, 2010.
- [72] Ling Long, *On Atkin and Swinnerton-Dyer congruence relations. III*, J. Number Theory **128** (2008), no. 8, 2413–2429. MR MR2394828
- [73] A. Marschner and J. Müller, *On a certain algebra of higher modular forms*, Algebra Colloq. **16** (2009), 371–380.
- [74] Barry Mazur, William Stein, and John Tate, *Computation of  $p$ -adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic). MR MR2290599

- [75] Marcel Mohyla and Gabor Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, 2009.
- [76] G. Nebe, *Kneser-Hecke-operators in coding theory*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 79–90. MR MR2293434 (2007m:11090)
- [77] Gabriele Nebe and Maria Teider, *Hecke actions on certain strongly modular genera of lattices*, Arch. Math. (Basel) **84** (2005), no. 1, 46–56. MR MR2106404 (2006c:11055)
- [78] Ken Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and  $q$ -series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR MR2020489 (2005c:11053)
- [79] Manabu Oura, Cris Poor, and David S. Yuen, *Towards the Siegel ring in genus four*, Int. J. Number Theory **4** (2008), no. 4, 563–586. MR MR2441792
- [80] Ariel Pacetti and Fernando Rodriguez Villegas, *Computing weight 2 modular forms of level  $p^2$* , Math. Comp. **74** (2005), no. 251, 1545–1557 (electronic), With an appendix by B. Gross. MR MR2137017 (2006a:11053)
- [81] Kathleen L. Petersen, *One-cusped congruence subgroups of Bianchi groups*, Math. Ann. **338** (2007), no. 2, 249–282. MR MR2302062 (2008b:20063)
- [82] Francesco Dalla Piazza and Bert van Geemen, *Siegel modular forms and finite symplectic groups*, 2008.
- [83] Robert Pollack, *On the  $p$ -adic  $L$ -function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558. MR MR1983040 (2004e:11050)
- [84] Alexandru A. Popa, *Central values of Rankin  $L$ -series over real quadratic fields*, Compos. Math. **142** (2006), no. 4, 811–866. MR MR2249532
- [85] Jordi Quer, *Fields of definition of building blocks*, Math. Comp. **78** (2009), no. 265, 537–554. MR MR2448720
- [86] Jeremy Rouse, *Bounds for the coefficients of powers of the Delta-function*, Bull. London Math. Soc. **40** (2008), no. 6, 1081–1090.
- [87] Emmanuel Royer, *Evaluating convolution sums of the divisor function with quasi-modular forms*, Int. J. Number Theory **3** (2007), no. 2, 231–261.

- [88] Michael M. Schein, *Weights in Serre's conjecture for Hilbert modular forms: the ramified case*, Israel J. Math. **166** (2008), 369–391. MR MR2430440
- [89] Mehmet Haluk Şengün, *The nonexistence of certain representations of the absolute Galois group of quadratic fields*, Proc. Amer. Math. Soc. **137** (2009), no. 1, 27–35. MR MR2439421
- [90] William Stein, *Modular Forms: A Computational Approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007, With an appendix by Paul E. Gunnells. MR MR2289048
- [91] William A. Stein, *Explicit Approaches to Modular Abelian Varieties*, PhD Thesis, University of California, Berkeley, 2000.
- [92] William A. Stein, *An introduction to computing modular forms using modular symbols*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 641–652. MR MR2467560 (2009k:11085)
- [93] William A. Stein and Helena A. Verrill, *Cuspidal modular symbols are transportable*, LMS J. Comput. Math. **4** (2001), 170–181 (electronic). MR MR1901355 (2003m:11074)
- [94] Helena A. Verrill, *Transportable modular symbols and the intersection pairing*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 219–233. MR MR2041086 (2005b:11063)
- [95] John Voight, *Computing fundamental domains for Fuchsian groups*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 469–491. MR MR2541438
- [96] Gabor Wiese, *Dihedral Galois representations and Katz modular forms*, Doc. Math. **9** (2004), 123–133 (electronic). MR MR2054983 (2005c:11065)
- [97] Gabor Wiese, *Modular Forms of Weight One over Finite Fields*, PhD Thesis, Universiteit Leiden, 2005.
- [98] Gabor Wiese, *On the faithfulness of parabolic cohomology as a Hecke module over a finite field*, J. reine angew. Math. **606** (2007), 79–103. MR MR2337642 (2008g:11092)

- [99] ———, *On projective linear groups over finite fields as Galois groups over the rational numbers*, Edixhoven, Bas et al., Modular forms on Schiermonnikoog. Based on the conference on modular forms, Schiermonnikoog, Netherlands, October 2006, Cambridge University Press, Cambridge, 2008, pp. 343–350. MR )
- [100] ———, *On modular symbols and the cohomology of Hecke triangle surfaces*, Int. J. Number Theory **5** (2009), no. 1, 89–108. MR MR2499023
- [101] Dan Yasaki, *Integral cohomology of certain Picard modular surfaces*, 2007.
- [102] Dan Yasaki, *Elliptic points of the Picard modular group*, Monatsh. Math. **156** (2009), no. 4, 391–396. MR MR2486605
- [103] Jahan Zahid, *Zeros of  $p$ -adic forms*, J. Number Theory **129** (2009), no. 10, 2439–2456. MR MR2541024
- [104] David Zywina, *A refinement of Koblitz’s conjecture*, 2009.

# Arithmetic Algebraic Geometry

11Gxx

- [1] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, 617–636. MR MR2251484 (2007c:11076)
- [2] Amod Agashe and William Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR MR1939144 (2003h:11070)
- [3] ———, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur. MR MR2085902 (2005g:11119)
- [4] Scott Ahlgren and Matthew Papanikolas, *Higher Weierstrass points on  $X_0(p)$* , Trans. Amer. Math. Soc. **355** (2003), no. 4, 1521–1535 (electronic). MR MR1946403 (2003j:11065)
- [5] Avner Ash, Darrin Doud, and David Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579. MR MR1896473 (2003g:11055)
- [6] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen, *Finiteness results for modular curves of genus at least 2*, Amer. J. Math. **127** (2005), no. 6, 1325–1387. MR MR2183527
- [7] Arthur Baragar and Ronald van Luijk,  *$K3$  surfaces with Picard number three and canonical vector heights*, Math. Comp. **76** (2007), no. 259, 1493–1498 (electronic). MR MR2299785
- [8] Mark Bauer, Edlyn Teske, and Annegret Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005 (electronic). MR MR2164107
- [9] Tobias Berger and Krzysztof Klosin, *A deformation problem for Galois representations over imaginary quadratic fields*, J. Inst. Math. Jussieu **8** (2009), no. 4, 669–692. MR MR2540877



- [10] Amnon Besser and Rob De Jeu, *li(p)-service? an algorithm for computing p-adic polyalgorithms*, *Math. Comp.* **77** (2008), no. 262, 1105–1134. MR MR2373194
- [11] Peter Birkner, *Efficient arithmetic on low-genus curves*, Ph D thesis, Technische Universiteit Eindhoven, 2009.
- [12] Nigel Boston and Rafe Jones, *Arboreal Galois representations*, *Geom. Dedicata* **124** (2007), 27–35. MR MR2318536
- [13] Irene I. Bouw and Brian Osserman, *Some 4-point Hurwitz numbers in positive characteristic*, 2009.
- [14] M. J. Bright, N. Bruin, E. V. Flynn, and A. Logan, *The Brauer-Manin obstruction and Sh[2]*, *LMS J. Comput. Math.* **10** (2007), 354–377 (electronic). MR MR2342713
- [15] David Brown, *The Chabauty-Coleman bound at a prime of bad reduction*, 2008.
- [16] ———, *Primitive integral solutions to  $x^2 + y^3 = z^{10}$* , 2009.
- [17] Ezra Brown and Bruce T. Myers, *Elliptic curves from Mordell to Diophantus and back*, *Amer. Math. Monthly* **109** (2002), no. 7, 639–649. MR MR1917222 (2003d:11080)
- [18] N. Bruin and E. V. Flynn, *n-covers of hyperelliptic curves*, *Math. Proc. Cambridge Philos. Soc.* **134** (2003), no. 3, 397–405. MR MR1981207 (2004b:11089)
- [19] Nils Bruin, *Visualising Sha[2] in abelian surfaces*, *Math. Comp.* **73** (2004), no. 247, 1459–1476 (electronic). MR MR2047096 (2005c:11067)
- [20] ———, *The arithmetic of Prym varieties in genus 3*, *Compos. Math.* **144** (2008), no. 2, 317–338. MR MR2406115
- [21] Nils Bruin and Kevin Doerksen, *The arithmetic of genus two curves with (4,4)-split Jacobians*, arXiv:0902.3480v2 (2010).
- [22] Nils Bruin and Noam D. Elkies, *Trinomials  $ax^7 + bx + c$  and  $ax^8 + bx + c$  with Galois groups of order 168 and  $8 \cdot 168$* , *Algorithmic Number Theory (Sydney, 2002)*, *Lecture Notes in Comput. Sci.*, vol. 2369, Springer, Berlin, 2002, pp. 172–188. MR MR2041082 (2005d:11094)

- [23] Nils Bruin and E. Victor Flynn, *Towers of 2-covers of hyperelliptic curves*, Trans. Amer. Math. Soc. **357** (2005), no. 11, 4329–4347 (electronic). MR MR2156713 (2006k:11118)
- [24] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884
- [25] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, 2008.
- [26] ———, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.
- [27] Armand Brumer and Kenneth Kramer, *Paramodular abelian varieties of odd conductor*, 2010.
- [28] Yann Bugeaud, Maurice Mignotte, Samir Siksek, Michael Stoll, and Szabolcs Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **2** (2008), no. 8, 859–885. MR MR2457355
- [29] Kevin Buzzard and L. J. P. Kilford, *The 2-adic eigencurve at the boundary of weight space*, Compos. Math. **141** (2005), no. 3, 605–619. MR MR2135280 (2005m:11101)
- [30] Robert Carls, *Theta null points of 2-adic canonical lifts*, 2005.
- [31] ———, *Explicit Frobenius lifts on elliptic curves*, 2009.
- [32] ———, *Fast point counting on genus two curves in characteristic three*, 2010.
- [33] Robert Carls and David Lubicz, *A  $p$ -adic quasi-quadratic time point counting algorithm*, Int. Math. Res. Not. IMRN (2009), no. 4, 698–735. MR MR2480098
- [34] Antoine Chambert-Loir, *Compter (rapidement) le nombre de solutions d'équations dans les corps finis*, 2006.
- [35] Denis Charles and Kristin Lauter, *Computing modular polynomials*, LMS J. Comput. Math. **8** (2005), 195–204 (electronic). MR MR2166572
- [36] Denis Xavier Charles, *Complex multiplication tests for elliptic curves*, 2004.
- [37] Imin Chen, *On the equation  $s^2 + y^{2p} = \alpha^3$* , Math. Comp. **77** (2008), no. 262, 1223–1227. MR MR2373199

- [38] Imin Chen and Chris Cummins, *Elliptic curves with nonsplit mod 11 representations*, Math. Comp. **73** (2004), no. 246, 869–880 (electronic). MR MR2031412 (2004m:11083)
- [39] Robert F. Coleman and William A. Stein, *Approximation of eigenforms of infinite slope by eigenforms of finite slope*, Geometric Aspects of Dwork Theory. Vol. I, II, Walter de Gruyter GmbH & Co. KG, Berlin, 2004, pp. 437–449. MR MR2023296 (2005h:11092)
- [40] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731. MR MR2183392 (2006m:11080)
- [41] Brian Conrad, Bas Edixhoven, and William Stein,  *$J_1(p)$  has connected fibers*, Doc. Math. **8** (2003), 331–408 (electronic). MR MR2029169 (2004k:11094)
- [42] Caterina Consani and Jasper Scholten, *Arithmetic on a quintic threefold*, Internat. J. Math. **12** (2001), no. 8, 943–972. MR MR1863287 (2002h:11058)
- [43] Patrick Kenneth Corn, *Del Pezzo Surfaces and the Brauer-Manin obstruction*, PhD Thesis, University of California, Berkley, 1998.
- [44] Gunther Cornelissen, Aristides Kontogeorgis, and Lotte van der Zalm, *Arithmetic equivalence for function fields, the Goss zeta function and a generalisation*, J. Number Theory **130** (2010), no. 4, 1000–1012. MR 2600417
- [45] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second ed., Cambridge University Press, Cambridge, 1997. MR MR1628193 (99e:11068)
- [46] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, *Explicit  $n$ -descent on elliptic curves. I. Algebra*, J. reine angew. Math. **615** (2008), 121–155. MR MR2384334
- [47] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon, and M. Stoll, *Explicit  $n$ -descent on elliptic curves, II: Geometry*, J. reine angew. Math **2009** (2009), no. 632, 63–84.
- [48] J. E. Cremona, T. A. Fisher, and M. Stoll, *Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves*, Algebra and Number Theory **4** (2010), no. 6, 763–820.
- [49] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR MR2367320 (2008k:11057)

- [50] J. E. Cremona, M. Prickett, and Samir Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68. MR MR2197860 (2006k:11121)
- [51] John Cremona, *The elliptic curve database for conductors to 130000*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 11–29. MR MR2282912 (2007k:11087)
- [52] John E. Cremona, *A solution for note 84.35*, The Mathematical Gazette **86** (2002), no. 505, 66–68.
- [53] John Cullinan, *A computational approach to the 2-torsion structure of abelian threefolds*, Math. Comp. **78** (2009), no. 267, 1825–1836. MR MR2501078
- [54] C. J. Cummins and S. Pauli, *Congruence subgroups of  $\mathrm{PSL}(2, Z)$  of genus less than or equal to 24*, Experiment. Math. **12** (2003), no. 2, 243–255. MR MR2016709 (2004i:11037)
- [55] Samit Dasgupta, *Computations of elliptic units for real quadratic fields*, Canad. J. Math. **59** (2007), no. 3, 553–574. MR MR2319158
- [56] Chantal David and Tom Weston, *Local torsion on elliptic curves and the deformation theory of Galois representations*, Math. Res. Lett. **15** (2008), no. 3, 599–611. MR MR2407234 (2009e:11109)
- [57] Christophe Delaunay and Christian Wuthrich, *Self-points on elliptic curves of prime conductor*, Int. J. Number Theory **5** (2009), no. 5, 911–932. MR MR2553516
- [58] Daniel Delbourgo and Thomas Ward, *The growth of CM periods over false Tate extensions*, Experiment. Math. **19** (2010), no. 2, 195–210. MR 2676748
- [59] Daniel Delbourgo and Tom Ward, *Non-abelian congruences between  $L$ -values of elliptic curves*, Ann. Inst. Fourier (Grenoble) **58** (2008), no. 3, 1023–1055. MR MR2427518 (2009i:11129)
- [60] Lassina Dembélé, *A non-solvable Galois extension of  $Q$  ramified at 2 only*, C. R. Math. Acad. Sci. Paris **347** (2009), no. 3-4, 111–116. MR MR2538094
- [61] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, 2009.

- [62] Jan Denef and Frederik Vercauteren, *An extension of Kedlaya's algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 308–323. MR MR2041093 (2005d:11088)
- [63] Xavier Charles Denis, *Complex multiplication tests for elliptic curves*, 2004.
- [64] Claus Diem and Emmanuel Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21** (2008), no. 4, 593–611. MR MR2438510
- [65] Luis Dieulefait, E. Gonzalez-Jimenez, and J. Jimenez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, arXiv:0909.1661v1 (2009).
- [66] T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 1, 211–272, With an appendix by J. Coates and R. Sujatha. MR MR2294995 (2008g:11106)
- [67] Tim Dokchitser and Vladimir Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 516–524. MR MR2418807
- [68] Tim Dokchitser and Vladimir Dokchitser, *A note on the Mordell-Weil rank modulo  $n$* , 2009.
- [69] Darrin Doud, *A procedure to calculate torsion of elliptic curves over  $\mathbf{Q}$* , Manuscripta Math. **95** (1998), no. 4, 463–469. MR MR1618198 (99c:11067)
- [70] Andrej Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III **42(62)** (2007), no. 1, 3–18. MR MR2332654 (2008e:11062)
- [71] S. Duquesne, *Rational points on hyperelliptic curves and an explicit Weierstrass preparation theorem*, Manuscripta Math. **108** (2002), no. 2, 191–204. MR MR1918586 (2003e:11067)
- [72] Sylvain Duquesne, *Points rationnels et méthode de Chabauty elliptique*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 99–113, Les XXIIèmes Journées Arithmétiques (Lille, 2001). MR MR2019003 (2005a:11074)
- [73] ———, *Elliptic curves associated with simplest quartic fields*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 81–100. MR MR2332055 (2008e:11063)

- [74] Sylvain Duquesne, *Montgomery ladder for all genus 2 curves in characteristic 2*, Arithmetic of Finite Fields, Lecture Notes in Computer Science, vol. 5130, Springer, 2008, pp. 174–188.
- [75] ———, *Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2*, Math. Comput. Sci. **3** (2010), no. 2, 173–183.
- [76] Bas Edixhoven, *On the computation of the coefficients of a modular form*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 30–39. MR MR2282913 (2007k:11085)
- [77] Kirsten Eisentraeger, Dimitar Jetchev, and Kristin Lauter, *On the computation of the Cassels pairing for certain Kolyvagin classes in the Shafarevich-Tate group*, 2008, pp. 113–125.
- [78] Kirsten Eisenträger and Kristin Lauter, *A CRT algorithm for constructing genus 2 curves over finite fields*, 2007.
- [79] Noam D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, 2007.
- [80] ———, *Shimura curve computations via K3 surfaces of Neron-Severi rank at least 19*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 196–211.
- [81] Noam D. Elkies and Mark Watkins, *Elliptic curves of large rank and small conductor*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 42–56. MR MR2137342 (2006c:11065)
- [82] Arsen Elkin, *Hyperelliptic Jacobians with real multiplication*, J. Number Theory **117** (2006), no. 1, 53–86. MR MR2204735 (2006j:11081)
- [83] Andreas-Stephan Elsenhans and Jörg Jahnel, *K3 surfaces of Picard rank one and degree two*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 212–225.
- [84] G. Everest and T. Ward, *The canonical height of an algebraic point on an elliptic curve*, New York J. Math. **6** (2000), 331–342 (electronic). MR MR1800354 (2001j:11056)

- [85] Graham Everest, Patrick Ingram, Valéry Mahé, and Shaun Stevens, *The uniform primality conjecture for elliptic curves*, Acta Arith. **134** (2008), no. 2, 157–181. MR MR2429645
- [86] Graham Everest, Patrick Ingram, and Shaun Stevens, *Primitive divisors on twists of Fermat’s cubic*, LMS J. Comput. Math. **12** (2009), 54–81. MR MR2486632
- [87] Graham Everest and Valéry Mahé, *A generalization of Siegel’s theorem and Hall’s conjecture*, Experiment. Math. **18** (2009), no. 1, 1–9. MR MR2548983
- [88] Graham Everest, Ouamporn Phuksuwan, and Shaun Stevens, *The uniform primality conjecture for the twisted Fermat cubic*, arXiv:1003.2131v2 (2010).
- [89] Xander Faber and Benjamin Hutz, *On the number of rational iterated pre-images of the origin under quadratic dynamical systems*, 2008.
- [90] Reza Rezaeian Farashahi and Ruud Pellikaan, *The quadratic extension extractor for (hyper)elliptic curves in odd characteristic*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 4547, Springer, Berlin, 2007, pp. 219–236. MR MR2387145 (2009a:11252)
- [91] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **To appear** (2010).
- [92] Julio Fernández, Josep González, and Joan-C. Lario, *Plane quartic twists of  $X(5, 3)$* , Canad. Math. Bull. **50** (2007), no. 2, 196–205. MR MR2317442 (2008b:11067)
- [93] Luís R. A. Finotti, *Degrees of the elliptic Teichmüller lift*, J. Number Theory **95** (2002), no. 2, 123–141. MR MR1924093 (2003m:11089)
- [94] ———, *Minimal degree liftings of hyperelliptic curves*, J. Math. Sci. Univ. Tokyo **11** (2004), no. 1, 1–47. MR MR2044910 (2005a:11087)
- [95] ———, *Minimal degree liftings in characteristic 2*, J. Pure Appl. Algebra **207** (2006), no. 3, 631–673. MR MR2265544 (2007g:11068)
- [96] ———, *Lifting the  $j$ -invariant: Questions of Mazur and Tate*, J. Number Theory **130** (2010), no. 3, 620–638.
- [97] Tom Fisher, *The Hessian of a genus one curve*, 2006.

- [98] ———, *Testing equivalence of ternary cubics*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 333–345. MR MR2282934 (2007j:11074)
- [99] ———, *A new approach to minimising binary quartics and ternary cubics*, Math. Res. Lett. **14** (2007), no. 4, 597–613. MR MR2335986 (2008k:11058)
- [100] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR MR2448246
- [101] ———, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138. MR MR2467841 (2009m:11078)
- [102] E. V. Flynn, *The Hasse principle and the Brauer-Manin obstruction for curves*, Manuscripta Math. **115** (2004), no. 4, 437–466. MR MR2103661 (2005j:11047)
- [103] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR MR2402033
- [104] E. V. Flynn and J. Wunderle, *Cycles of covers*, Monatsh. Math. **Online first** (2008), 16.
- [105] David Freeman, Peter Stevenhagen, and Marco Streng, *Abelian varieties with prescribed embedding degree*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 60–73.
- [106] S. D. Galbraith, J. F. McKee, and P. C. Valença, *Ordinary abelian varieties having small embedding degree*, Finite Fields Appl. **13** (2007), no. 4, 800–814. MR MR2359321
- [107] Steven D. Galbraith, *Weil descent of Jacobians*, Discrete Appl. Math. **128** (2003), no. 1, 165–180, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991424 (2004m:14046)
- [108] Irene García-Selfa, Enrique González-Jiménez, and José M. Tornero, *Galois theory, discriminants and torsion subgroup of elliptic curves*, J. Pure Appl. Algebra **214** (2010), no. 8, 1340–1346. MR 2593667 (2011b:11076)
- [109] P. Gaudry and É. Schost, *Modular equations for hyperelliptic curves*, Math. Comp. **74** (2005), no. 249, 429–454 (electronic). MR MR2085901 (2006b:11062)



- [110] Pierrick Gaudry, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, 2004.
- [111] Pierrick Gaudry and Robert Harley, *Counting points on hyperelliptic curves over finite fields*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 313–332. MR MR1850614 (2002f:11072)
- [112] Eknath Ghate, Enrique González-Jiménez, and Jordi Quer, *On the Brauer class of modular endomorphism algebras*, Int. Math. Res. Not. (2005), no. 12, 701–723. MR MR2146605 (2006b:11058)
- [113] Jean Gillibert, *Invariants de classes: exemples de non-annulation en dimension supérieure*, Math. Ann. **338** (2007), no. 2, 475–495. MR MR2302072 (2008c:11089)
- [114] Edray Goins, *Explicit descent via 4-isogeny on an elliptic curve*, 2004.
- [115] Josep González and Jordi Guàrdia, *Genus two curves with quaternionic multiplication and modular Jacobian*, Math. Comp. **78** (2009), no. 265, 575–589. MR MR2448722
- [116] Josep González, Jordi Guàrdia, and Victor Rotger, *Abelian surfaces of  $GL_2$ -type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287. MR MR2114780 (2005m:11107)
- [117] Josep González and Victor Rotger, *Non-elliptic Shimura curves of genus one*, J. Math. Soc. Japan **58** (2006), no. 4, 927–948. MR MR2276174 (2007k:11093)
- [118] Enrique González-Jiménez, Josep González, and Jordi Guàrdia, *Computations on modular Jacobian surfaces*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 189–197. MR MR2041083 (2005c:11074)
- [119] Enrique González-Jiménez and Roger Oyono, *Non-hyperelliptic modular curves of genus 3*, J. Number Theory **130** (2010), no. 4, 862–878. MR 2600407
- [120] Enrique Gonzalez-Jimenez and Xavier Xarles, *Five squares in arithmetic progression over quadratic fields*, 2009.
- [121] ———, *On symmetric square values of quadratic polynomials*, 2010.
- [122] Eyal Z. Goren and Kristin E. Lauter, *The distance between superspecial abelian varieties with real multiplication*, J. Number Theory **129** (2009), no. 6, 1562–1578. MR MR2521493

- [123] Eyal Z. Goren and Kristin E. Lauter, *Genus 2 curves with complex multiplication*, arXiv:1003.4759v1 (2010).
- [124] Matthew Greenberg, *Computing Heegner points arising from Shimura curve parametrizations*, 2006.
- [125] ———, *Heegner point computations via numerical  $p$ -adic integration*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 4076, Springer Berlin / Heidelberg, 2006, pp. 361–376.
- [126] ———, *Heegner Points and Rigid Analytic Modular Forms*, PhD Thesis, McGill University, 2006.
- [127] Grigor Grigorov, Andrei Jorza, Stephan Patrikis, William A. Stein, and Corina Tarnita-Patrascu, *Verification of the Birch and Swinnerton-Dyer conjecture for specific elliptic curves*.
- [128] Jordi Guàrdia, *Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves*, Ann. Inst. Fourier (Grenoble) **57** (2007), no. 4, 1253–1283. MR MR2339331 (2008g:11105)
- [129] Brian Hansen, *Explicit computations supporting a generalization of Serre’s conjecture*, MSc, Brigham Young University, 2005.
- [130] Robin Hartshorne and Ronald van Luijk, *Non-Euclidean Pythagorean triples, a problem of Euler, and rational points on  $K3$  surfaces*, Math. Intelligencer **30** (2008), no. 4, 4–10. MR MR2501390
- [131] Ki-ichiro Hashimoto, Katsuya Miyake, and Hiroaki Nakamura (eds.), *Galois Theory and Modular Forms*, Developments in Mathematics, vol. 11, Boston, MA, Kluwer Academic Publishers, 2004. MR MR2059977 (2004k:11003)
- [132] Brendan Hassett, Anthony Vàrilly-Alvarado, and Patrick Varilly, *Transcendental obstructions to weak approximation on general  $K3$  surfaces*, 2010.
- [133] Florian Hess, *Computing relations in divisor class groups of algebraic curves over finite fields*, 2003.
- [134] ———, *A note on the Tate pairing of curves over finite fields*, Arch. Math. (Basel) **82** (2004), no. 1, 28–32. MR MR2034467 (2004m:14040)

- [135] Laura Hitt, *Families of genus 2 curves with small embedding degree*, J. Math. Cryptol. **3** (2009), no. 1, 19–36. MR MR2524253
- [136] E. W. Howe and K. E. Lauter, *Improved upper bounds for the number of points on curves over finite fields*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 6, 1677–1737. MR MR2038778 (2005c:11079)
- [137] Everett W. Howe, *Infinite families of pairs of curves over  $Q$  with isomorphic Jacobians*, J. London Math. Soc. (2) **72** (2005), no. 2, 327–350. MR MR2156657 (2006b:11064)
- [138] ———, *Supersingular genus-2 curves over fields of characteristic 3*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 49–69. MR MR2459989 (2009j:11103)
- [139] Everett W. Howe, Kristin E. Lauter, and Jaap Top, *Pointless curves of genus three and four*, Arithmetic, Geometry and Coding Theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 125–141. MR MR2182840 (2006g:11125)
- [140] Everett W. Howe and Hui June Zhu, *On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field*, J. Number Theory **92** (2002), no. 1, 139–163. MR MR1880590 (2003g:11063)
- [141] Hendrik Hubrechts, *Point counting in families of hyperelliptic curves*, Found. Comput. Math. **8** (2008), no. 1, 137–169. MR MR2403533
- [142] ———, *Quasi-quadratic elliptic curve point counting using rigid cohomology*, J. Symb. Comput. **44** (2009), no. 9, 1255–1267.
- [143] Klaus Hulek and Helena Verrill, *On modularity of rigid and nonrigid Calabi-Yau varieties associated to the root lattice  $A_4$* , Nagoya Math. J. **179** (2005), 103–146. MR MR2164402
- [144] Klaus Hulek and Helena A. Verrill, *On the motive of Kummer varieties associated to  $\Gamma_1(7)$  — Supplement to the paper: “The modularity of certain non-rigid Calabi-Yau threefolds” by R. Livné and N. Yui*, J. Math. Kyoto Univ. **45** (2005), no. 4, 667–681. MR MR2226624 (2007b:11092)
- [145] Patrick Ingram, *Multiples of integral points on elliptic curves*, J. Number Theory **129** (2009), no. 1, 182–208. MR MR2468477 (2010a:11102)

- [146] Farzali A. Izadi and V. Kumar Murty, *Counting points on an abelian variety over a finite field*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 323–333. MR MR2092391 (2005f:11127)
- [147] David Jao and Vladimir Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 219–233.
- [148] Dimitar Jetchev, Kristin Lauter, and William Stein, *Explicit Heegner points: Kolyvagin’s conjecture and non-trivial elements in the Shafarevich-Tate group*, J. Number Theory **129** (2009), no. 2, 284 – 302.
- [149] Dimitar P. Jetchev and William A. Stein, *Visibility of the Shafarevich-Tate group at higher level*, Doc. Math. **12** (2007), 673–696. MR MR2377239
- [150] Jorge Jimenez-Urroz and Tonghai Yang, *Heegner zeros of theta functions*, Trans. Amer. Math. Soc. **355** (2003), no. 10, 4137–4149 (electronic). MR MR1990579 (2005e:11070)
- [151] Rafe Jones and Jeremy Rouse, *Galois theory of iterated endomorphisms*, Proc. London Math. Soc. (3) **100** (2010), 763–794.
- [152] David Joyner and Amy Ksir, *Modular representations on some Riemann-Roch spaces of modular curves  $X(N)$* , Computational Aspects of Algebraic Curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 163–205. MR MR2182040 (2006k:11112)
- [153] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.
- [154] Koray Karabina and Edlyn Teske, *On prime-order elliptic curves with embedding degrees  $k=3,4$ , and 6*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 102–117.
- [155] L. J. P. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms*, J. Number Theory **97** (2002), no. 1, 157–164. MR MR1939142 (2003j:11046)
- [156] ———, *Slopes of 2-adic overconvergent modular forms with small level*, Math. Res. Lett. **11** (2004), no. 5-6, 723–739. MR MR2106238 (2005h:11093)
- [157] L. J. P. Kilford, *On a  $p$ -adic extension of the Jacquet-Langlands correspondence to weight 1*, 2008.

- [158] David R. Kohel, *Hecke module structure of quaternions*, Class Field Theory—Its Centenary and Prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 177–195. MR MR1846458 (2002i:11059)
- [159] ———, *The AGM- $X_0(N)$  Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)
- [160] David R. Kohel and William A. Stein, *Component groups of quotients of  $J_0(N)$* , Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 405–412. MR MR1850621 (2002h:11051)
- [161] David R. Kohel and Helena A. Verrill, *Fundamental domains for Shimura curves*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 205–222, Les XXIIèmes Journées Arithmétiques (Lille, 2001). MR MR2019012 (2004k:11096)
- [162] Kenji Koike and Annegret Weng, *Construction of CM Picard curves*, Math. Comp. **74** (2005), no. 249, 499–518 (electronic). MR MR2085904 (2005g:11103)
- [163] Aristides Kontogeorgis and Victor Rotger, *On the non-existence of exceptional automorphisms on Shimura curves*, Bull. Lond. Math. Soc. **40** (2008), no. 3, 363–374. MR MR2418792
- [164] Andrew Kresch and Yuri Tschinkel, *Integral points on punctured abelian surfaces*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 198–204. MR MR2041084 (2005d:11081)
- [165] L. Kulesz, G. Matera, and É. Schost, *Uniform bounds on the number of rational points of a family of curves of genus 2*, J. Number Theory **108** (2004), no. 2, 241–267. MR MR2098638 (2005h:11130)
- [166] Dominic Lanphier, *The trace of special values of modular  $L$ -functions*.
- [167] Alan G. B. Lauder, *Ranks of elliptic curves over function fields*, LMS J. Comput. Math. **11** (2008), 172–212. MR MR2429996
- [168] Alan G.B. Lauder, *Degenerations and limit Frobenius structures in rigid cohomology*, 2009.

- [169] F. Leprévost, M. Pohst, and A. Schöpp, *Rational torsion of  $J_0(N)$  for hyperelliptic modular curves and families of Jacobians of genus 2 and genus 3 curves with a rational point of order 5, 7 or 10*, Abh. Math. Sem. Univ. Hamburg **74** (2004), 193–203. MR MR2112831 (2005h:11131)
- [170] Franck Leprévost, Michael Pohst, and Andreas Schöpp, *Familles de polynômes liées aux courbes modulaires  $X(l)$  unicursales et points rationnels non-triviaux de courbes elliptiques quotient*, Acta Arith. **110** (2003), no. 4, 401–410. MR MR2011317 (2004j:11053)
- [171] Reynald Lercier and David Lubicz, *A quasi-quadratic time algorithm for hyperelliptic curve point counting*, Ramanujan J. **12** (2006), no. 3, 399–423. MR MR2293798 (2008b:11069)
- [172] Reynald Lercier and Thomas Sirvent, *On Elkies subgroups of  $l$ -torsion points in elliptic curves defined over a finite field*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 783–797. MR MR2523317
- [173] Petr Lisoněk, *On the connection between Kloosterman sums and elliptic curves*, Sequences and Their Applications – SETA 2008: Proceedings (Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, eds.), Lecture Notes in Computer Science, vol. 5203, Springer, Berlin Heidelberg, 2008, pp. 182–187.
- [174] Adam Logan and Ronald van Luijk, *Nontrivial elements of  $Sha$  explained through  $K3$  surfaces*, Math. Comp. **78** (2009), no. 265, 441–483. MR MR2448716
- [175] Ling Long and Chris Kurth, *On modular forms for some noncongruence subgroups of  $SL_2\mathbb{Z}$  II*, 2008.
- [176] Dino Lorenzini and Thomas J. Tucker, *Thue equations and the method of Coleman-Chabauty*, 2000.
- [177] Álvaro Lozano-Robledo, *On the product of twists of rank two and a conjecture of Larsen*, Ramanujan J. **19** (2009), no. 1, 53–61. MR MR2501236 (2010b:11062)
- [178] Kazuo Matsuno, *Construction of elliptic curves with large Iwasawa  $\lambda$ -invariants and large Tate-Shafarevich groups*, Manuscripta Math. **122** (2007), no. 3, 289–304. MR MR2305419

- [179] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)
- [180] J. Miret, R. Moreno, A. Rio, and M. Valls, *Computing the  $l$ -power torsion of an elliptic curve over a finite field*, Math. Comp. **78** (2009), no. 267, 1767–1786. MR MR2501074
- [181] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls, *Computing the height of volcanoes of  $l$ -isogenies of elliptic curves over finite fields*, Appl. Math. Comput. **196** (2008), no. 1, 67–76. MR MR2382590 (2008m:11122)
- [182] Josep M. Miret, Jordi Pujolàs, and Anna Rio, *Bisection for genus 2 curves in odd characteristic*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), no. 4, 55–60. MR MR2517297 (2010d:14039)
- [183] Jan-Steffen Müller, *Explicit Kummer surface theory for arbitrary characteristic*, London Math. Soc. J. Comput. Math. **13** (2010), 47–64.
- [184] Filip Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), no. 9, 1964–1968. MR 2653208
- [185] Annika Niehage, *Quantum Goppa codes over hyperelliptic curves*, Diplomarbeit, Universität Mannheim, 2004.
- [186] Ekin Ozman, *Local points on quadratic twists of  $X_0(N)$* , 2009.
- [187] Mihran Papikian, *On the degree of modular parametrizations over function fields*, J. Number Theory **97** (2002), no. 2, 317–349. MR MR1942964 (2004c:11104)
- [188] ———, *On the variation of Tate-Shafarevich groups of elliptic curves over hyperelliptic curves*, J. Number Theory **115** (2005), no. 2, 249–283. MR MR2180501 (2006g:11111)
- [189] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en  $p$* , Experiment. Math. **12** (2003), no. 2, 155–186. MR MR2016704 (2005h:11138)

- [190] Bjorn Poonen, *Computational aspects of curves of genus at least 2*, Algorithmic Number Theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 283–306. MR MR1446520 (98c:11059)
- [191] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of  $X(7)$  and primitive solutions to  $x^2 + y^3 = z^7$* , Duke Math. J. **137** (2007), no. 1, 103–158. MR MR2309145
- [192] Lisa Marie Redekop, *Torsion Points of Low Order on Elliptic Curves and Drinfeld Modules*, Ph.D. thesis, 2002, p. 95.
- [193] Jonathan Reynolds, *Extending Siegel’s theorem for elliptic curves*, Phd thesis, University of East Anglia, 2008.
- [194] Guillaume Ricotta and Thomas Vidick, *Hauteur asymptotique des points de Heegner*, Canad. J. Math. **60** (2008), no. 6, 1406–1436. MR MR2462452
- [195] Christophe Ritzenthaler, *Automorphismes des courbes modulaires  $X(n)$  en caractéristique  $p$* , Manuscripta Math. **109** (2002), no. 1, 49–62. MR MR1931207 (2003g:11067)
- [196] ———, *Point counting on genus 3 non hyperelliptic curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 379–394. MR MR2138009 (2006d:11065)
- [197] Christophe Ritzenthaler, *Explicit computations of Serre’s obstruction for genus 3 curves and application to optimal curves*, LMS Journal of Computation and Mathematics **13** (2010), 192–207.
- [198] Mohammad Sadek, *Counting models of genus one curves*, 2010.
- [199] David Savitt, *The maximum number of points on a curve of genus 4 over  $F_8$  is 25*, Canad. J. Math. **55** (2003), no. 2, 331–352, With an appendix by Kristin Lauter. MR MR1969795 (2004i:11059)
- [200] Edward F. Schaefer and Michael Stoll, *How to do a  $p$ -descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231 (electronic). MR MR2021618 (2004g:11045)
- [201] Jasper Scholten, *Weil restriction of an elliptic curve over a quadratic extension*, 2004.



- [202] Andreas M. Schöpp, *Über torsionspunkte elliptischer und hyperelliptischer kurven nebst anwendungen*, Ph.D. thesis, Technische Universitaet Berlin,, April 2005, p. 92.
- [203] Samir Siksek, *On standardized models of isogenous elliptic curves*, Math. Comp. **74** (2005), no. 250, 949–951 (electronic). MR MR2114657 (2005i:11076)
- [204] ———, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236. MR MR2491943 (2010b:11069)
- [205] Samir Siksek and John E. Cremona, *On the Diophantine equation  $x^2 + 7 = y^m$* , Acta Arith. **109** (2003), no. 2, 143–149. MR MR1980642 (2004c:11109)
- [206] Samir Siksek and Michael Stoll, *On a problem of Hajdu and Tengely*, 2009.
- [207] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 163–180.
- [208] ———, *Families of explicit isogenies of hyperelliptic Jacobians*, Arithmetic, Geometry, Cryptography and Coding Theory, Contemporary Mathematics, vol. 521, AMS, Providence, R.I., 2009, pp. 121–144.
- [209] Sebastian Karl Michael Stamminger, *Explicit 8-descent on elliptic curves*, Ph.D. thesis, International University Bremen, 2005, p. 107.
- [210] William Stein, *Studying the Birch and Swinnerton-Dyer conjecture for modular abelian varieties using Magma*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 93–116. MR MR2278924
- [211] William A. Stein, *There are genus one curves over  $Q$  of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147. MR MR1900139 (2003c:11059)
- [212] ———, *Shafarevich-Tate groups of nonsquare order*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 277–289. MR MR2058655 (2005c:11072)
- [213] ———, *Visibility of Mordell-Weil groups*, Doc. Math. **12** (2007), 587–606. MR MR2377241 (2009a:11128)
- [214] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR MR1829626 (2002b:11089)

- [215] ———, *On the height constant for curves of genus two. II*, Acta Arith. **104** (2002), no. 2, 165–182. MR MR1914251 (2003f:11093)
- [216] Michael Stoll, *Rational 6-cycles under iteration of quadratic polynomials*, LMS J. Comput. Math. **11** (2008), 367–380.
- [217] Fritz Grunewald Tatiana Bandman, Shelly Garion, *On the surjectivity of engel words on  $psl(2,q)$* , 2010, pp. 1–22.
- [218] Thotsaphon Thongjunthug, *Computing a lower bound for the canonical height on elliptic curves over totally real number fields*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 139–152.
- [219] Hans-Christian Graf v. Bothmer, *Finite field experiments (with an appendix by Stefan Wiedmann)*, Higher-Dimensional Geometry over Finite Fields, NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 16, IOS Press, 2008, pp. 1–62.
- [220] Anthony Vàrilly-Alvarado and Bianca Viray, *Failure of the Hasse principle for Enriques surfaces*, Advances in Mathematics **226** (2011), 4884–4901.
- [221] Marie-France Vignéras,  *$p$ -adic integral structures of some representations of  $GL(2, F)$* , 2005.
- [222] Bogdan G. Vioreanu, *Mordell-Weil problem for cubic surfaces, numerical evidence*, 2008.
- [223] Bianca Viray, *A family of varieties with exactly one pointless rational fiber*, 2009.
- [224] Mark Watkins, *A note on integral points on elliptic curves*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 707–720. MR MR2330437 (2008e:11069)
- [225] Mark Watkins, *Some remarks on Heegner point computations*, 2006.
- [226] Mark Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125. MR MR2410120
- [227] Rolf Stefan Wilke, *On rational embeddings of curves in the second Garcia-Stichtenoth tower*, Finite Fields Appl. **14** (2008), no. 2, 494–504. MR MR2401990 (2009a:11131)
- [228] Christian Wuthrich, *The fine Tate-Shafarevich group*, Math. Proc. Cambridge Philos. Soc. **142** (2007), no. 1, 1–12. MR MR2296386 (2008b:11064)

- [229] ———, *Self-points on an elliptic curve of conductor 14*, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, RIMS Kôkyûroku Bessatsu, B4, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007, pp. 189–195. MR MR2402010 (2009e:11112)
- [230] Chaoping Xing, *Applications of algebraic curves to constructions of sequences*, Cryptography and Computational Number Theory (Singapore, 1999), Progr. Comput. Sci. Appl. Logic, vol. 20, Birkhäuser, Basel, 2001, pp. 137–146. MR MR1944725 (2004e:11068)
- [231] Chaoping Xing and Sze Ling Yeo, *Construction of global function fields from linear codes and vice versa*, Trans. Amer. Math. Soc. **361** (2008), no. 3, 1333–1349.
- [232] Huilin Zhu and Jianhua Chen, *Integral points on a class of elliptic curve*, Wuhan Univ. J. Nat. Sci. **11** (2006), no. 3, 477–480. MR MR2258847 (2007d:11064)

# Geometry of Numbers

11Hxx

- [1] Kanat Abdukhalikov, *Unimodular Hermitian lattices*, Mathematisches Forschungsinstitut Oberwolfach Report No. 1/2005 (2005), 27–30.
- [2] Kanat Abdukhalikov and Rudolf Scharlau, *Unimodular lattices in dimensions 14 and 15 over the Eisenstein integers*, Math. Comp. **78** (2009), no. 265, 387–403. MR MR2448712
- [3] Christine Bachoc and Gabriele Nebe, *Classification of two genera of 32-dimensional lattices of rank 8 over the Hurwitz order*, Experiment. Math. **6** (1997), no. 2, 151–162. MR MR1474575 (98g:11078)
- [4] Christine Bachoc and Boris Venkov, *Modular forms, lattices and spherical designs*, Réseaux Euclidiens, Designs Sphériques et Formes Modulaires, Monogr. Enseign. Math., vol. 37, Enseignement Math., Geneva, 2001, pp. 87–111. MR MR1878746 (2003d:11096)
- [5] Werner Backes and Susanne Wetzel, *Heuristics on lattice basis reduction in practice*, ACM J. Exp. Algorithmics **7** (2002), 21 pp. (electronic), Fourth Workshop on Algorithm Engineering (Saarbrücken, 2000). MR MR1973646 (2004c:68162)
- [6] Siegfried Boecherer and Gabriele Nebe, *On theta series attached to maximal lattices and their adjoints*, 2009.
- [7] Robin Chapman, Steven T. Dougherty, Philippe Gaborit, and Patrick Solé, *2-modular lattices from ternary codes*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 73–85. MR MR1925991 (2004g:94091)
- [8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. MR MR1662447 (2000b:11077)
- [9] R. Coulangeon, M. I. Icaza, and M. O’Ryan, *Lenstra’s constant and extreme forms in number fields*, Experiment. Math. **16** (2007), no. 4, 455–462. MR MR2378486 (2008m:11131)

- [10] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin, *A generalization of Voronoi's reduction theory and its application*, Duke Math. J. **142** (2008), no. 1, 127–164. MR MR2397885 (2009a:11141)
- [11] C. Fieker and M. E. Pohst, *On lattices over number fields*, Algorithmic Number Theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 133–139. MR MR1446505 (98g:11079)
- [12] Philippe Gaborit, *Construction of new extremal unimodular lattices*, European J. Combin. **25** (2004), no. 4, 549–564. MR MR2069381 (2006a:11088)
- [13] Paul E. Gunnells and Dan Yasaki, *Perfect forms over totally real number fields*, 2009.
- [14] Masaaki Harada, *On the existence of frames of the Niemeier lattices and self-dual codes over  $F_p$* , J. Algebra **321** (2009), no. 8, 2345–2352. MR MR2501524 (2010c:94066)
- [15] Masaaki Harada, Masaaki Kitazume, and Michio Ozeki, *Ternary code construction of unimodular lattices and self-dual codes over  $Z_6$* , J. Algebraic Combin. **16** (2002), no. 2, 209–223. MR MR1943589 (2004b:11099)
- [16] Boris Hemkemeier, *Algorithmische konstruktionen von gittern*, 2004.
- [17] Jacques Martinet and Achill Schürmann, *On classifying Minkowskian sublattices*, 2009.
- [18] G. Nebe, *Kneser-Hecke-operators in coding theory*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 79–90. MR MR2293434 (2007m:11090)
- [19] Gabriele Nebe, *Finite quaternionic matrix groups*, Represent. Theory **2** (1998), 106–223 (electronic). MR MR1615333 (99f:20085)
- [20] ———, *Even lattices with covering radius  $< \sqrt{2}$* , Beiträge Algebra Geom. **44** (2003), no. 1, 229–234. MR MR1990996 (2004c:11120)
- [21] ———, *Strongly modular lattices with long shadow*, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 187–196. MR MR2145580 (2006c:11077)
- [22] Gabriele Nebe, *An even unimodular 72-dimensional lattice of minimum 8*, 2010.
- [23] Gabriele Nebe and Kristina Schindelar, *S-extremal strongly modular lattices*, J. Théor. Nombres Bordeaux **19** (2007), no. 3, 683–701. MR MR2388794

- [24] Gabriele Nebe and Boris Venkov, *The strongly perfect lattices of dimension 10*, J. Théor. Nombres Bordeaux **12** (2000), no. 2, 503–518, Colloque International de Théorie des Nombres (Talence, 1999). MR MR1823200 (2002f:11081)
- [25] ———, *Low-dimensional strongly perfect lattices I: The 12-dimensional case*, Enseign. Math. (2) **51** (2005), no. 1-2, 129–163. MR MR2154624 (2006b:11069)
- [26] Gabriele Nebe and Boris Venkov, *Low dimensional strongly perfect lattices III: Dual strongly perfect lattices of dimension 14*, IJNT **2** (2010), no. 2, 387–409.
- [27] Gabriele Nebe and Chaoping Xing, *A Gilbert-Varshamov type bound for Euclidean packings*, Math. Comp. **77** (2008), no. 264, 2339–2344. MR MR2429888
- [28] Phong Q. Nguyen and Damien Stehlé, *LLL on the average*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 238–256. MR MR2282928 (2008a:11154)
- [29] W. Plesken and M. Pohst, *Constructing integral lattices with prescribed minimum. I*, Math. Comp. **45** (1985), no. 171, 209–221, S5–S16. MR MR790654 (87e:11077)
- [30] ———, *Constructing integral lattices with prescribed minimum. II*, Math. Comp. **60** (1993), no. 202, 817–825. MR MR1176715 (93h:11070)
- [31] E. M. Rains and N. J. A. Sloane, *The shadow theory of modular and unimodular lattices*, J. Number Theory **73** (1998), no. 2, 359–389. MR MR1657980 (99i:11053)
- [32] Achill Schürmann, *Enumerating perfect forms*, Proceedings of the International Conference on Quadratic Forms, Chile 2007, Contemporary Mathematics, vol. To appear, 2009.
- [33] ———, *Perfect, strongly eutactic lattices are periodic extreme*, Adv. Math **225** (2010), no. 5, 2546–2564.
- [34] Achill Schürmann and Frank Vallentin, *Local covering optimality of lattices: Leech lattice versus root lattice  $E_8$* , Int. Math. Res. Not. (2005), no. 32, 1937–1955. MR MR2173600 (2006i:11076)
- [35] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin, *Classification of eight-dimensional perfect forms*, Electron. Res. Announc. Amer. Math. Soc. **13** (2007), 21–32 (electronic). MR MR2300003

- [36] N. J. A. Sloane, R. H. Hardin, T. D. S. Duff, and J. H. Conway, *Minimal-energy clusters of hard spheres*, *Discrete Comput. Geom.* **14** (1995), no. 3, 237–259. MR MR1344734 (96m:52033)
- [37] Anthony Várilly-Alvarado and David Zywina, *Arithmetic  $E_8$  lattices with maximal Galois action*, *LMS J. Comput. Math.* **12** (2009), 144–165. MR MR2559115

# Probabilistic Theory

11Kxx

- [1] Wieb Bosma, Karma Dajani, and Cor Kraaikamp, *Entropy quotients and correct digits in number-theoretic expansions*, Dynamics and Stochastics, IMS Lecture Notes Monogr. Ser., vol. 48, Inst. Math. Statist., Beachwood, OH, 2006, pp. 176–188. MR MR2306199



# Zeta and $L$ -functions: Analytic Theory

11Mxx

- [1] Peter Borwein, Greg Fee, Ron Ferguson, and Alexa van der Waall, *Zeros of partial sums of the Riemann zeta function*, Experiment. Math. **16** (2007), no. 1, 21–39. MR MR2312975 (2008a:11099)
- [2] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731. MR MR2183392 (2006m:11080)
- [3] Gunther Cornelissen, Aristides Kontogeorgis, and Lotte van der Zalm, *Arithmetic equivalence for function fields, the Goss zeta function and a generalisation*, J. Number Theory **130** (2010), no. 4, 1000–1012. MR 2600417
- [4] M. P. F. du Sautoy, J. J. McDermott, and G. C. Smith, *Zeta functions of crystallographic groups and analytic continuation*, Proc. London Math. Soc. (3) **79** (1999), no. 3, 511–534. MR MR1710163 (2000k:11103)
- [5] Marcus du Sautoy and Luke Woodward, *Nilpotent groups: Explicit examples*, Zeta Functions of Groups and Rings, Lecture Notes in Computer Science, vol. 1925/2008, Springer Berlin / Heidelberg, 2008, pp. 21–68.
- [6] Ralf Gerkmann, *Relative rigid cohomology and deformation of hypersurfaces*, Int. Math. Res. Pap. IMRP (2007), no. 1, Art. ID rpm003, 67. MR MR2334009
- [7] Kiran S. Kedlaya and Andrew V. Sutherland, *Computing  $L$ -series of hyperelliptic curves*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, 2008, pp. 312–326.
- [8] Emmanuel Kowalski, *The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros*, Int. Math. Res. Not. IMRN (2008), Art. ID rnn 091, 57. MR MR2439552
- [9] Alan G. B. Lauder, *A recursive method for computing zeta functions of varieties*, LMS J. Comput. Math. **9** (2006), 222–269 (electronic). MR MR2261044 (2007g:14022)
- [10] Phil Martin and Mark Watkins, *Symmetric powers of elliptic curve  $L$ -functions*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 377–392. MR MR2282937 (2007i:11087)

- [11] Moritz Minzloff, *Computing zeta functions of superelliptic curves in larger characteristic*, Math. Comput. Sci. **3** (2010), 209–224.
- [12] Christopher Voll, *Normal subgroup growth in free class-2-nilpotent groups*, Math. Ann. **332** (2005), no. 1, 67–79. MR MR2139251
- [13] Alexey Zaytsev and Gary McGuire, *On the zeta functions of an optimal tower of function fields over  $F_4$* , 2009.

# Additive and Multiplicative Number Theory

11Pxx, 11Nxx

- [1] Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), no. 259, 1683–1690 (electronic). MR MR2299795 (2007m:11170)
- [2] Wieb Bosma and Ben Kane, *The Aliquot constant*, 2009.
- [3] Javier Cilleruelo, *The least common multiple of a quadratic sequence*, Compositio Mathematica **To appear** (2010).
- [4] H. Dubner, T. Forbes, N. Lygeros, M. Mizony, H. Nelson, and P. Zimmermann, *Ten consecutive primes in arithmetic progression*, Math. Comp. **71** (2002), no. 239, 1323–1328 (electronic). MR MR1898760 (2003d:11137)
- [5] Sharon Anne Garthwaite, *Convolution congruences for the partition function*, Proc. Amer. Math. Soc. **135** (2007), no. 1, 13–20 (electronic). MR MR2280169
- [6] F. G. Garvan, *Biranks for partitions into 2 colors*, 2009.
- [7] David Zywina, *A refinement of Koblitz’s conjecture*, 2009.

# Algebraic Number Theory

11Rxx and 11Sxx

- [1] Avner Ash, Jos Brakenhoff, and Theodore Zarrabi, *Equality of polynomial and field discriminants*, Experiment. Math. **16** (2007), no. 3, 367–374. MR MR2367325 (2008i:11129)
- [2] Laurent Bartholdi and Michael R. Bush, *Maximal unramified 3-extensions of imaginary quadratic fields and  $SL_2(\mathbb{Z}_3)$* , J. Number Theory **124** (2007), no. 1, 159–166. MR MR2320997 (2008c:11153)
- [3] Ingrid Bauer, Fabrizio Catanese, and Fritz Grunewald, *The absolute Galois group acts faithfully on the connected components of the moduli space of surfaces of general type*, 2007.
- [4] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high three-rank*, Math. Comp. **77** (2008), no. 261, 503–530 (electronic). MR MR2353964
- [5] Amnon Besser and Rob De Jeu, *li(p)-service? an algorithm for computing p-adic polyalgorithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. MR MR2373194
- [6] Wieb Bosma, *Canonical bases for cyclotomic fields*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), no. 2, 125–134. MR MR1325517 (95k:11135)
- [7] ———, *Computation of cyclotomic polynomials with Magma*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 213–225. MR MR1344932 (96j:11142)
- [8] Wieb Bosma and Bart de Smit, *On arithmetically equivalent number fields of small degree*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 67–79. MR MR2041074 (2005e:11169)
- [9] Wieb Bosma and Peter Stevenhagen, *On the computation of quadratic 2-class groups*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313. MR MR1438471 (98e:11129a)
- [10] Nigel Boston, *Galois p-groups unramified at p—a survey*, Primes and knots, Contemp. Math., vol. 416, Amer. Math. Soc., Providence, RI, 2006, pp. 31–40. MR MR2276134 (2007k:11191)

- [11] ———, *Galois groups of tamely ramified  $p$ -extensions*, J. Théor. Nombres Bordeaux **19** (2007), no. 1, 59–70. MR MR2332053
- [12] Nigel Boston and Rafe Jones, *Arboreal Galois representations*, Geom. Dedicata **124** (2007), 27–35. MR MR2318536
- [13] Nigel Boston and Charles Leedham-Green, *Counterexamples to a conjecture of Lemmermeyer*, Arch. Math. (Basel) **72** (1999), no. 3, 177–179. MR MR1671275 (99m:11131)
- [14] M. R. Bush, *Computation of Galois groups associated to the 2-class towers of some quadratic fields*, J. Number Theory **100** (2003), no. 2, 313–325. MR MR1978459 (2004f:11130)
- [15] Nigel P. Byott, James E. Carter, Cornelius Greither, and Henri Johnston, *On the restricted hilbert-speiser and leopoldt properties*, Illinois J. Math **To appear** (2011).
- [16] Murat Cenk and Ferruh Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010), no. 2, 172–186.
- [17] H. Cohen, F. Diaz y Diaz, and M. Olivier, *Subexponential algorithms for class group and unit computations*, J. Symbolic Comput. **24** (1997), no. 3-4, 433–441, Computational algebra and number theory (London, 1993). MR MR1484490 (98m:11138)
- [18] Henri Cohen, *A survey of computational class field theory*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 1–13, Les XXèmes Journées Arithmétiques (Limoges, 1997). MR MR1730429 (2000j:11169)
- [19] B. de Smit and H. W. Lenstra, Jr., *Linearly equivalent actions of solvable groups*, J. Algebra **228** (2000), no. 1, 270–285. MR MR1760965 (2001f:20069)
- [20] Bart de Smit, *On arithmetically equivalent fields with distinct  $p$ -class numbers*, J. Algebra **272** (2004), no. 2, 417–424. MR MR2028064 (2005f:11252)
- [21] Bart de Smit and Robert Perlis, *Zeta functions do not determine class numbers*, Bull. Amer. Math. Soc. (N.S.) **31** (1994), no. 2, 213–215. MR MR1260520 (95a:11100)
- [22] Daniel Delbourgo and Thomas Ward, *The growth of CM periods over false Tate extensions*, Experiment. Math. **19** (2010), no. 2, 195–210. MR 2676748

- [23] Daniel Delbourgo and Tom Ward, *Non-abelian congruences between  $L$ -values of elliptic curves*, Ann. Inst. Fourier (Grenoble) **58** (2008), no. 3, 1023–1055. MR MR2427518 (2009i:11129)
- [24] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, 2009.
- [25] Darrin Doud, *Supersingular Galois representations and a generalization of a conjecture of Serre*, Experiment. Math. **16** (2007), no. 1, 119–128. MR MR2312982 (2007m:11076)
- [26] Kirsten Eisenträger and Kristin Lauter, *Computing Igusa class polynomials via the chinese remainder theory*, 2004.
- [27] Jordan S. Ellenberg and Akshay Venkatesh, *The number of extensions of a number field with fixed degree and bounded discriminant*, Ann. of Math. (2) **163** (2006), no. 2, 723–741. MR MR2199231 (2006j:11159)
- [28] Claus Fieker, *Applications of the class field theory of global fields*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 31–62. MR MR2278922
- [29] ———, *Sparse representation for cyclotomic fields*, Experiment. Math. **16** (2007), no. 4, 493–500. MR MR2378488
- [30] ———, *Minimizing representations over number fields II. Computations in the Brauer group*, J. Algebra **322** (2009), no. 3, 752–765. MR MR2531221
- [31] Claus Fieker and Michael E. Pohst, *Dependency of units in number fields*, Math. Comp. **75** (2006), no. 255, 1507–1518 (electronic). MR MR2219041 (2007a:11168)
- [32] ———, *A lower regulator bound for number fields*, J. Number Theory **128** (2008), no. 10, 2767–2775. MR MR2441075
- [33] Felix Fontein, *The infrastructure of a global field of arbitrary unit rank*, 2008.
- [34] David Ford, Sebastian Pauli, and Xavier-François Roblot, *A fast algorithm for polynomial factorization over  $Q_p$* , J. Théor. Nombres Bordeaux **14** (2002), no. 1, 151–169. MR MR1925995 (2003g:11134)

- [35] Robert Fraatz, *On the computation of integral closures of cyclic extensions of function fields*, LMS J. Comput. Math. **10** (2007), 141–160 (electronic). MR MR2308855 (2008b:11123)
- [36] Irene García-Selfa, Enrique González-Jiménez, and José M. Tornero, *Galois theory, discriminants and torsion subgroup of elliptic curves*, J. Pure Appl. Algebra **214** (2010), no. 8, 1340–1346. MR 2593667 (2011b:11076)
- [37] S. P. Glasby, *Generators for the group of units of  $Z_n$* , Austral. Math. Soc. Gaz. **22** (1995), no. 5, 226–228. MR MR1378923 (97a:11199)
- [38] Norbert Goeb, *Computing the automorphism groups of hyperelliptic function fields*, 2003.
- [39] Ralph Greenberg, *On the structure of certain Galois cohomology groups*, Doc. Math. (2006), no. Extra Vol., 335–391 (electronic). MR MR2290593 (2008b:11112)
- [40] J. Guardia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428v1 (2009).
- [41] Jordi Guardia, Jesus Montes, and Enric Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, 2008.
- [42] Lajos Hajdu, *Optimal systems of fundamental  $S$ -units for LLL-reduction*, Period. Math. Hungar. **59** (2009), no. 1, 53–79. MR MR2544620
- [43] Emmanuel Hallouin and Christian Maire, *Cancellation in totally definite quaternion algebras*, J. Reine Angew. Math. **595** (2006), 189–213. MR MR2244802 (2007g:11146)
- [44] Emmanuel Hallouin and Marc Perret, *On the kernel of the norm in some unramified number fields extensions*, 2007.
- [45] Stephan Hell, *Die nenner des kontsevich-integrals und ein spezieller drinfeld-assoziator*, Ph.D. thesis, Freie Universität Berlin, July 2002, p. 92.
- [46] F. Hess, *An algorithm for computing isomorphisms of algebraic function fields*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 263–271. MR MR2137359
- [47] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. **72** (2003), no. 243, 1531–1548 (electronic). MR MR1972751 (2004f:11126)

- [48] David Hubbard, *Dihedral side extensions and class groups*, J. Number Theory **128** (2008), no. 4, 731–737. MR MR2400036
- [49] Jean-François Jaulent, Sebastian Pauli, Michael E. Pohst, and Florence Soriano-Gafiuk, *Computation of 2-groups of positive classes of exceptional number fields*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 715–732. MR MR2523314
- [50] ———, *Computation of 2-groups of narrow logarithmic divisor classes of number fields*, J. Symbolic Comput. **44** (2009), no. 7, 852–863. MR MR2522586 (2010d:11133)
- [51] Henri Johnston, *On the trace map between absolutely abelian number fields of equal conductor*, Acta Arith. **122** (2006), no. 1, 63–74. MR MR2217325 (2006k:11203)
- [52] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR MR2194887 (2006k:11230)
- [53] John Jossey, *Galois 2-extensions unramified outside 2*, J. Number Theory **124** (2007), no. 1, 42–56. MR MR2320990
- [54] Masanari Kida, *Kummer theory for norm algebraic tori*, J. Algebra **293** (2005), no. 2, 427–447. MR MR2172348 (2007h:14061)
- [55] Masanari Kida, *Descent Kummer theory via Weil restriction of multiplicative groups*, J. of Number Theory **130** (2010), no. 3, 639–659.
- [56] ———, *A Kummer theoretic construction of an  $S_3$ -polynomial with given quadratic subfield*, Interdisciplinary Information Sciences **16** (2010), no. 1, 17–20.
- [57] Masanari Kida, Guénaél Renault, and Kazuhiro Yokoyama, *Quintic polynomials of Hashimoto-Tsunogai, Brumer and Kummer*, Int. J. Number Theory **5** (2009), no. 4, 555–571. MR MR2532276
- [58] Masanari Kida, Yuichi Rikuna, and Atsushi Sato, *Classifying Brumer’s quintic polynomials by weak Mordell-Weil groups*, IJNT **6** (2010), no. 3, 691–704.
- [59] Norbert Klíngen, *Leopoldt’s conjecture for imaginary Galois number fields*, J. Symbolic Comput. **10** (1990), no. 6, 531–545. MR MR1087978 (92e:11124)
- [60] Jürgen Klíners and Gunter Malle, *Counting nilpotent Galois extensions*, J. Reine Angew. Math. **572** (2004), 1–26. MR MR2076117 (2005f:11259)



- [61] Jürgen Klüners and Sebastian Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), no. 1, 47–64. MR MR2166795
- [62] Elisavet Konstantinou and Aristides Kontogeorgis, *Computing polynomials of the Ramanujan  $t_n$  class invariants*, Canad. Math. Bull. **52** (2009), no. 4, 583–597. MR MR2567152
- [63] M. Künzer and H. Weber, *Some additive Galois cohomology rings*, Comm. Algebra **33** (2005), no. 12, 4415–4455. MR MR2188320 (2006k:11221)
- [64] Matthias Künzer and Eduard Wirsing, *On coefficient valuations of Eisenstein polynomials*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 801–823. MR MR2212127 (2006m:11151)
- [65] Thorsten Lagemann, *Codes und automorphismen optimaler artin-schreier-turme*, Ph.D. thesis, Ruprecht-Karls-Universität Heidelberg, April 2006, p. 92.
- [66] Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field*, Experiment. Math. **12** (2003), no. 2, 211–225. MR MR2016707 (2004j:11143)
- [67] Franck Leprévost, Michael Pohst, and Andreas Schöpp, *Units in some parametric families of quartic fields*, Acta Arith. **127** (2007), no. 3, 205–216. MR MR2310343 (2008a:11133)
- [68] Aaron Levin, *Ideal class groups and torsion in Picard groups of varieties*, 2008.
- [69] Melissa L. Macasieb, *Derived arithmetic Fuchsian groups of genus two*, Experiment. Math. **17** (2008), no. 3, 347–369. MR MR2455706 (2009i:11135)
- [70] Piotr Maciak, *Primes of the form  $x^2 + n * y^2$  in function fields*, 2009.
- [71] Kazuo Matsuno, *Construction of elliptic curves with large Iwasawa  $\lambda$ -invariants and large Tate-Shafarevich groups*, Manuscripta Math. **122** (2007), no. 3, 289–304. MR MR2305419
- [72] William G. McCallum and Romyar T. Sharifi, *A cup product in the Galois cohomology of number fields*, Duke Math. J. **120** (2003), no. 2, 269–310. MR MR2019977 (2004j:11136)

- [73] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group  $c_2 \times c_2 \times c_2$* , Journal of Number Theory **129** (2009), no. 1, 231 – 245.
- [74] Sebastian Pauli, *Efficient enumeration of extensions of local fields with bounded discriminant*, Ph.D. thesis, Concordia University, June 2001, p. 82.
- [75] Sebastian Pauli, *Constructing class fields over local fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 627–652. MR MR2330432 (2008f:11135)
- [76] Sebastian Pauli and Florence Soriano-Gafiuk, *The discrete logarithm in logarithmic  $l$ -class groups and its applications in  $K$ -theory*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 367–378. MR MR2138008 (2006a:11155)
- [77] Diana Savin, *About certain prime numbers*, 2009, p. 9.
- [78] René Schoof, *Arakelov class groups and ideal lattices*, 2005, pp. 23–24.
- [79] René Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 447–495. MR MR2467554
- [80] Andreas M. Schöpp, *Fundamental units in a parametric family of not totally real quintic number fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 693–706. MR MR2330436 (2008f:11121)
- [81] Romyar T. Sharifi, *Iwasawa theory and the Eisenstein ideal*, Duke Math. J. **137** (2007), no. 1, 63–101. MR MR2309144
- [82] ———, *On Galois groups of unramified pro- $p$  extensions*, Math. Ann. **342** (2008), no. 2, 297–308. MR MR2425144
- [83] William Stein and Yan Zhang, *On power bases in number fields*, 2005.
- [84] Aliza Steurer, *On the Galois groups of the 2-class towers of some imaginary quadratic fields*, J. Number Theory **125** (2007), no. 1, 235–246. MR MR2333129
- [85] Mark van Hoeij and John Cremona, *Solving conics over function fields*, J. Théor. Nombres Bordeaux **18** (2006), no. 3, 595–606. MR MR2330429 (2008f:11133)

- [86] Stéphane Vinatier, *Structure galoisienne dans les extensions faiblement ramifiées de  $Q$* , J. Number Theory **91** (2001), no. 1, 126–152. MR MR1869322 (2002h:11112)
- [87] John Voight, *The gauss higher relative class number problem*, Ann. Sci. Math. Québec **Accepted** (2009).
- [88] Gabor Wiese, *On projective linear groups over finite fields as Galois groups over the rational numbers*, Edixhoven, Bas et al., Modular forms on Schiermonnikoog. Based on the conference on modular forms, Schiermonnikoog, Netherlands, October 2006, Cambridge University Press, Cambridge, 2008, pp. 343–350. MR )
- [89] Qingquan Wu and Renate Scheidler, *An explicit treatment of biquadratic function fields*, Contrib. Discrete Math. **2** (2007), no. 1, 43–60 (electronic). MR MR2291883 (2008a:11144)
- [90] Dan Yasaki, *Binary Hermitian forms over a cyclotomic field*, J. Algebra **322** (2009), no. 11, 4132–4142. MR MR2556143
- [91] Alexey Zaytsev and Gary McGuire, *On the zeta functions of an optimal tower of function fields over  $F_4$* , 2009.

# Finite Fields

11Txx

- [1] R. D. Baker, G. L. Ebert, K. H. Leung, and Q. Xiang, *A trace conjecture and flag-transitive affine planes*, J. Combin. Theory Ser. A **95** (2001), no. 1, 158–168. MR MR1840482 (2002c:11166)
- [2] Aart Blokhuis, Robert S. Coulter, Marie Henderson, and Christine M. O’Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 37–42. MR MR1849077 (2002e:11175)
- [3] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *A few more quadratic APN functions*, 2008.
- [4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. **14** (2008), no. 3, 703–714. MR MR2435056
- [5] Marcus Brinkmann and Gregor Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 273–288. MR MR2438456
- [6] Jessica F. Burkhart, Neil J. Calkin, Shuhong Gao, Justine C. Hyde-Volpe, Kevin James, Hiren Maharaj, Shelly Manber, Jared Ruiz, and Ethan Smith, *Finite field elements of high order arising from modular curves*, Des. Codes Cryptogr. **51** (2009), no. 3, 301–314. MR MR2485499 (2010b:11164)
- [7] Murat Cenk and Ferruh Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010), no. 2, 172–186.
- [8] Mihai Cipu, *Dickson polynomials that are permutations*, Serdica Math. J. **30** (2004), no. 2-3, 177–194. MR MR2098331 (2005g:11244)
- [9] Mihai Cipu and Stephen D. Cohen, *Dickson polynomial permutations*, Finite Fields and Applications, Contemporary Mathematics, vol. 461, 2008.
- [10] Stephen D. Cohen, *Finite field elements with specified order and traces*, Des. Codes Cryptogr. **36** (2005), no. 3, 331–340. MR MR2163064
- [11] ———, *Primitive polynomials with a prescribed coefficient*, Finite Fields Appl. **12** (2006), no. 3, 425–491. MR MR2229326 (2007e:11141)

- [12] Robert S. Coulter, George Havas, and Marie Henderson, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's  $p^s$ -polynomials*, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput, vol. 9, World Sci. Publ., River Edge, NJ, 2001, pp. 36–45. MR MR1877440 (2002m:11103)
- [13] ———, *On decomposition of sub-linearised polynomials*, J. Aust. Math. Soc. **76** (2004), no. 3, 317–328. MR MR2053506 (2005b:13013)
- [14] Robert S. Coulter and Marie Henderson, *The compositional inverse of a class of permutation polynomials over a finite field*, Bull. Austral. Math. Soc. **65** (2002), no. 3, 521–526. MR MR1910505 (2003f:11185)
- [15] Jean-Marc Couveignes and Reynald Lercier, *Elliptic periods for finite fields*, Finite Fields Appl. **15** (2009), no. 1, 1–22. MR MR2468989 (2009j:12006)
- [16] Yves Edel and Alexander Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), no. 1, 59–81. MR MR2476525 (2010c:11154)
- [17] Ronald Evans, Henk D. L. Hollmann, Christian Krattenthaler, and Qing Xiang, *Gauss sums, Jacobi sums, and  $p$ -ranks of cyclic difference sets*, J. Combin. Theory Ser. A **87** (1999), no. 1, 74–119. MR MR1698269 (2001b:05038)
- [18] Reza Rezaeian Farashahi and Ruud Pellikaan, *The quadratic extension extractor for (hyper)elliptic curves in odd characteristic*, Arithmetic of finite fields, Lecture Notes in Comput. Sci., vol. 4547, Springer, Berlin, 2007, pp. 219–236. MR MR2387145 (2009a:11252)
- [19] Kseniya Garaschuk, *On binary and ternary Kloosterman sums*, Ph D thesis, Simon Fraser University, 2007.
- [20] Lenwood S. Heath and Nicholas A. Loehr, *New algorithms for generating Conway polynomials over finite fields*, Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (Baltimore, MD, 1999) (New York), ACM, 1999, pp. 429–437. MR MR1739972 (2000j:11187)
- [21] Dae San Kim, *Codes associated with  $O^+(2n, 2^r)$  and power moments of Kloosterman sums*, 2008.
- [22] ———, *Codes associated with orthogonal groups and power moments of Kloosterman sums*, 2008.

- [23] ———, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums*, 2008.
- [24] Douglas A. Leonard, *A weighted module view of integral closures of affine domains of type I*, *Adv. Math. Commun.* **3** (2009), no. 1, 1–11.
- [25] Petr Lisoněk, *On the connection between Kloosterman sums and elliptic curves*, *Sequences and Their Applications – SETA 2008: Proceedings* (Solomon W. Golomb, Matthew G. Parker, Alexander Pott, and Arne Winterhof, eds.), *Lecture Notes in Computer Science*, vol. 5203, Springer, Berlin Heidelberg, 2008, pp. 182–187.
- [26] Marko Moisio, *Kloosterman sums, elliptic curves, and irreducible polynomials with prescribed trace and norm*, *Acta Arith.* **132** (2008), no. 4, 329–350. MR MR2413356 (2009f:11149)
- [27] Ferruh Özbudak, *Elements of prescribed order, prescribed traces and systems of rational functions over finite fields*, *Des. Codes Cryptogr.* **34** (2005), no. 1, 35–54. MR MR2126576 (2005k:11239)
- [28] B. V. Petrenko, *On the product of two primitive elements of maximal subfields of a finite field*, *J. Pure Appl. Algebra* **178** (2003), no. 3, 297–306. MR MR1953735 (2004b:11165)
- [29] ———, *On the sum of two primitive elements of maximal subfields of a finite field*, *Finite Fields Appl.* **9** (2003), no. 1, 102–116. MR MR1954786 (2003m:12004)
- [30] Håvard Raddum and Igor Semaev, *Solving multiple right hand sides linear equations*, *Des. Codes Cryptogr.* **49** (2008), no. 1-3, 147–160. MR MR2438447

# Computational Methods

11-04 and 11Yxx

- [1] Fadwa S. Abu Muriefah, Florian Luca, and Alain Togbé, *On the Diophantine equation  $x^2 + 5^a 13^b = y^n$* , *Glasg. Math. J.* **50** (2008), no. 1, 175–181. MR MR2381741 (2008m:11071)
- [2] Fatima K. Abu Salem and Kamal Khuri-Makdisi, *Fast Jacobian group operations for  $C_{3,4}$  curves over a large finite field*, *LMS J. Comput. Math.* **10** (2007), 307–328 (electronic). MR MR2335723
- [3] Ali Akhavi and Damien Stehlé, *Speeding-up lattice reduction with random projections (extended abstract)*, *LATIN 2008: Theoretical informatics, Lecture Notes in Comput. Sci.*, vol. 4957, Springer, Berlin, 2008, pp. 293–305. MR MR2472745
- [4] Bill Allombert, *An efficient algorithm for the computation of Galois automorphisms*, *Math. Comp.* **73** (2004), no. 245, 359–375 (electronic). MR MR2034127 (2004k:11193)
- [5] Roberto Maria Avanzi, *Another look at square roots (and other less common operations) in fields of even characteristic*, *Selected Areas in Cryptography, Lecture Notes in Computer Science*, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 138–154.
- [6] Eric Bach and Denis Charles, *The hardness of computing an eigenform*, *Computational arithmetic geometry, Contemp. Math.*, vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 9–15. MR MR2459985 (2009i:11051)
- [7] Werner Backes and Susanne Wetzels, *An efficient LLL gram using buffered transformations*, *Computer Algebra in Scientific Computing, Lecture Notes in Computer Science*, vol. 4770/2007, Springer Berlin / Heidelberg, 2007, pp. 31–44.
- [8] David H. Bailey, Jonathan M. Borwein, Vishaal Kapoor, and Eric W. Weisstein, *Ten problems in experimental mathematics*, *Amer. Math. Monthly* **113** (2006), no. 6, 481–509. MR MR2231135 (2007b:65001)
- [9] Stéphane Ballet, *Quasi-optimal algorithms for multiplication in the extensions of  $\mathbf{F}_{16}$  of degree 13, 14 and 15*, *J. Pure Appl. Algebra* **171** (2002), no. 2-3, 149–164. MR MR1904474 (2003b:11133)

- [10] M. Bauer, M. J. Jacobson, Jr., Y. Lee, and R. Scheidler, *Construction of hyperelliptic function fields of high three-rank*, Math. Comp. **77** (2008), no. 261, 503–530 (electronic). MR MR2353964
- [11] Michael Beck, Eric Pine, Wayne Tarrant, and Kim Yarbrough Jensen, *New integer representations as the sum of three cubes*, Math. Comp. **76** (2007), no. 259, 1683–1690 (electronic). MR MR2299795 (2007m:11170)
- [12] Daniel J. Bernstein, *Batch binary edwards*, Advances in Cryptology - CRYPTO 2009, Lecture Notes in Comput. Sci., vol. 5677, Springer, Berlin, 2009, pp. 317–336.
- [13] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, Progress in cryptology—INDOCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4859, Springer, Berlin, 2007, pp. 167–182. MR MR2570254
- [14] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *ECM using Edwards curves*, 2008.
- [15] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 29–50.
- [16] Amnon Besser and Rob De Jeu, *li(p)-service? an algorithm for computing p-adic polyalgorithms*, Math. Comp. **77** (2008), no. 262, 1105–1134. MR MR2373194
- [17] Peter Birkner, *Efficient divisor class halving on genus two curves*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4356, Springer, Berlin/Heidelberg, pp. 317–326.
- [18] Werner Bley and Robert Boltje, *Computation of locally free class groups*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 72–86. MR MR2282916
- [19] Jonathan Borwein and David Bailey, *Mathematics by Experiment*, A K Peters Ltd., Natick, MA, 2004, Plausible reasoning in the 21st century. MR MR2033012 (2005b:00012)
- [20] Wieb Bosma, *Some computational experiments in number theory*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 1–30. MR MR2278921



- [21] Wieb Bosma, John Cannon, and Allan Steel, *Lattices of compatibly embedded finite fields*, J. Symbolic Comput. **24** (1997), no. 3-4, 351–369, Computational algebra and number theory (London, 1993). MR MR1484485 (99a:11143)
- [22] Wieb Bosma and Bart de Smit, *Class number relations from a computational point of view*, J. Symbolic Comput. **31** (2001), no. 1-2, 97–112, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806209 (2002a:11144)
- [23] ———, *On arithmetically equivalent number fields of small degree*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 67–79. MR MR2041074 (2005e:11169)
- [24] Wieb Bosma and Ben Kane, *The Aliquot constant*, 2009.
- [25] Wieb Bosma and Arjen K. Lenstra, *An implementation of the elliptic curve integer factorization method*, Computational Algebra and Number Theory (Sydney, 1992), Math. Appl., vol. 325, Kluwer Acad. Publ., Dordrecht, 1995, pp. 119–136. MR MR1344926 (96d:11134)
- [26] Wieb Bosma and Peter Stevenhagen, *Density computations for real quadratic units*, Math. Comp. **65** (1996), no. 215, 1327–1337. MR MR1344607 (96j:11171)
- [27] Johan Bosman, *On the computation of Galois representations associated to level one modular forms*, 2007.
- [28] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, Finite Fields and Applications, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 40–58. MR MR2092621
- [29] Aaron Bradord, Michael Monagan, and Colin Percival, *Integer factorization and computing discrete logarithms in Maple*, Proceedings of the 2006 Maple Conference, 2006, pp. 2–13.
- [30] Richard P. Brent, *Factorization of the tenth Fermat number*, Math. Comp. **68** (1999), no. 225, 429–451. MR MR1489968 (99e:11154)
- [31] ———, *Recent progress and prospects for integer factorisation algorithms*, Computing and Combinatorics (Sydney, 2000), Lecture Notes in Comput. Sci., vol. 1858, Springer, Berlin, 2000, pp. 3–22. MR MR1866110 (2002h:11138)

- [32] ———, *Note on Marsaglia's xorshift random number generators*, J. Stat. Soft **11** (2004), no. 5, 1–5.
- [33] Nils Bruin and Michael Stoll, *Deciding existence of rational points on curves: an experiment*, Experiment. Math. **17** (2008), no. 2, 181–189. MR MR2433884
- [34] Nils Bruin and Michael Stoll, *Two-cover descent on hyperelliptic curves*, 2008.
- [35] ———, *The Mordell-Weil sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math **13** (2010), 272–306.
- [36] David G. Cantor and Daniel M. Gordon, *Factoring polynomials over  $p$ -adic fields*, Algorithmic Number Theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 185–208. MR MR1850606 (2002f:11175)
- [37] Robert Carls, *Explicit Frobenius lifts on elliptic curves*, 2009.
- [38] ———, *Fast point counting on genus two curves in characteristic three*, 2010.
- [39] Wouter Castryck, Hendrik Hubrechts, and Frederik Vercauteren, *Computing zeta functions in families of  $C_{a,b}$  curves using deformation*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 296–311.
- [40] Antoine Chambert-Loir, *Compter (rapidement) le nombre de solutions d'équations dans les corps finis*, 2006.
- [41] Hugo Chapdelaine, *Computation of  $p$ -units in ray class fields of real quadratic number fields*, Math. Comp. **78** (2009), 2307–2345.
- [42] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit  $n$ -descent on elliptic curves. I. Algebra*, J. reine angew. Math. **615** (2008), 121–155. MR MR2384334
- [43] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. **72** (2003), no. 243, 1417–1441 (electronic). MR MR1972744 (2004a:11137)
- [44] M. Daberkow, *Computing with subfields*, J. Symbolic Comput. **24** (1997), no. 3–4, 371–384, Computational algebra and number theory (London, 1993). MR MR1484486 (98k:11185)

- [45] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörning, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Computational algebra and number theory (London, 1993). MR MR1484479 (99g:11150)
- [46] Lassina Dembélé, *Quaternionic Manin symbols, Brandt matrices, and Hilbert modular forms*, Math. Comp. **76** (2007), no. 258, 1039–1057 (electronic). MR MR2291849
- [47] Lassina Dembélé, *On the computation of algebraic modular forms on compact inner forms of  $GSp_4$* , 2009.
- [48] Lassina Dembélé and Steve Donnelly, *Computing Hilbert modular forms over fields with nontrivial class group*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 371–386. MR MR2467859 (2010d:11149)
- [49] Francisco Diaz y Diaz, Jean-François Jaulent, Sebastian Pauli, Michael Pohst, and Florence Soriano-Gafiuk, *A new algorithm for the computation of logarithmic  $l$ -class groups of number fields*, Experiment. Math. **14** (2005), no. 1, 65–74. MR MR2146520 (2006d:11154)
- [50] Claus Diem, *The GHS attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32. MR MR1966526 (2004a:14030)
- [51] ———, *Index calculus in class groups of plane curves of small degree*, 2005.
- [52] ———, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557. MR MR2282948
- [53] Jintai Ding, Jason E. Gower, and Dieter S. Schmidt, *Zhuang-Zi: A new algorithm for solving multivariate polynomial equations over a finite field*, 2006.
- [54] Jacques Dubrois and Jean-Guillaume Dumas, *Efficient polynomial time algorithms computing industrial-strength primitive roots*, Inform. Process. Lett. **97** (2006), no. 2, 41–45. MR MR2187046 (2006h:68064)
- [55] Sylvain Duquesne, *Montgomery ladder for all genus 2 curves in characteristic 2*, Arithmetic of Finite Fields, Lecture Notes in Computer Science, vol. 5130, Springer, 2008, pp. 174–188.

- [56] I. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, Advances in Cryptology—Asiacrypt'99 (Singapore), Lecture Notes in Comput. Sci., vol. 1716, Springer, Berlin, 1999, pp. 103–121. MR MR1773225
- [57] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **To appear** (2010).
- [58] Claus Fieker, *Applications of the class field theory of global fields*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 31–62. MR MR2278922
- [59] ———, *Sparse representation for cyclotomic fields*, Experiment. Math. **16** (2007), no. 4, 493–500. MR MR2378488
- [60] Claus Fieker and Willem A. de Graaf, *Finding integral linear dependencies of algebraic numbers and algebraic Lie algebras*, LMS J. Comput. Math. **10** (2007), 271–287 (electronic). MR MR2320832 (2008f:11119)
- [61] Claus Fieker and Michael E. Pohst, *Dependency of units in number fields*, Math. Comp. **75** (2006), no. 255, 1507–1518 (electronic). MR MR2219041 (2007a:11168)
- [62] Tom Fisher, *The Hessian of a genus one curve*, 2006.
- [63] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR MR2448246
- [64] ———, *Some improvements to 4-descent on an elliptic curve*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 125–138. MR MR2467841 (2009m:11078)
- [65] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR MR2402033
- [66] Felix Fontein, *The infrastructure of a global field of arbitrary unit rank*, 2008.
- [67] Robert Fraatz, *Computation of maximal orders of cyclic extensions of function fields*, PhD Thesis, Technischen Universität Berlin, 2005.
- [68] David Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, Pairing-based cryptography—Pairing 2007, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, pp. 152–176. MR MR2423638

- [69] David Mandell Freeman and Takakazu Satoh, *Constructing pairing-friendly hyperelliptic curves using Weil restriction*, 2010, pp. 1–31.
- [70] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46. MR MR1880933 (2003b:14032)
- [71] Pierrick Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology—Eurocrypt 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34. MR MR1772021
- [72] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya’s point-counting algorithm to superelliptic curves*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494. MR MR1934859 (2003h:11159)
- [73] Pierrick Gaudry, Alexander Kruppa, and Paul Zimmermann, *A GMP-based implementation of Schönhage-Strassen’s large integer multiplication algorithm*, ISSAC 2007, ACM, New York, 2007, pp. 167–174. MR MR2396199
- [74] Willi Geiselmann, Jörn Müller-Quade, and Rainer Steinwandt, *Comment on: “A new representation of elements of finite fields  $\text{GF}(2^m)$  yielding small complexity arithmetic circuits” by G. Drolet*, IEEE Trans. Comput. **51** (2002), no. 12, 1460–1461. MR MR2012149
- [75] Willi Geiselmann and Rainer Steinwandt, *A redundant representation of  $\text{GF}(q^n)$  for designing arithmetic circuits*, IEEE Trans. Comp **52** (2003), no. 7, 848–853.
- [76] ———, *Non-wafer-scale sieving hardware for the NFS: another attempt to cope with 1024-bit*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 466–481. MR MR2449226 (2009h:94125)
- [77] Martine Girard and Leopoldo Kulesz, *Computation of sets of rational points of genus-3 curves via the Demjanenko-Manin method*, LMS J. Comput. Math. **8** (2005), 267–300 (electronic). MR MR2193214
- [78] Norbert Goeb, *Computing the automorphism groups of hyperelliptic function fields*, 2003.

- [79] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarnita, *Computational verification of the birch and swinnerton-dyer conjecture for individual elliptic curves*, *Math. Comp.* **78** (2009), 2397–2425.
- [80] J. Guardia, J. Montes, and E. Nart, *Higher Newton polygons and integral bases*, arXiv:0902.3428v1 (2009).
- [81] Jordi Guardia, Jesus Montes, and Enric Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, 2008.
- [82] Lajos Hajdu, *Optimal systems of fundamental  $S$ -units for LLL-reduction*, *Period. Math. Hungar.* **59** (2009), no. 1, 53–79. MR MR2544620
- [83] G. Hanrot and F. Morain, *Solvability by radicals from an algorithmic point of view*, *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation* (New York), ACM, 2001, pp. 175–182 (electronic). MR MR2049746 (2005a:11200)
- [84] Guillaume Hanrot and Damien Stehlé, *Improved analysis of Kannan’s shortest lattice vector algorithm (extended abstract)*, *Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci.*, vol. 4622, Springer, Berlin, 2007, pp. 170–186. MR MR2419600
- [85] David Harvey, *Kedlaya’s algorithm in larger characteristic*, *Int. Math. Res. Not. IMRN* (2007), no. 22, Art. ID rnm095, 29. MR MR2376210
- [86] ———, *A cache-friendly truncated FFT*, *Theor. Comput. Sci.* **410** (2009), no. 27–29, 2649–2658.
- [87] Lenwood S. Heath and Nicholas A. Loehr, *New algorithms for generating Conway polynomials over finite fields*, *J. Symbolic Comput.* **38** (2004), no. 2, 1003–1024. MR MR2093563 (2005g:11247)
- [88] F. Hess, *Weil descent attacks*, *Advances in Elliptic Curve Cryptography*, *London Math. Soc. Lecture Note Ser.*, vol. 317, Cambridge Univ. Press, Cambridge, 2005, pp. 151–180. MR MR2169214
- [89] Florian Hess, Sebastian Pauli, and Michael E. Pohst, *Computing the multiplicative group of residue class rings*, *Math. Comp.* **72** (2003), no. 243, 1531–1548 (electronic). MR MR1972751 (2004f:11126)

- [90] Hendrik Hubrechts, *Point counting in families of hyperelliptic curves*, Found. Comput. Math. **8** (2008), no. 1, 137–169. MR MR2403533
- [91] ———, *Quasi-quadratic elliptic curve point counting using rigid cohomology*, J. Symb. Comput. **44** (2009), no. 9, 1255–1267.
- [92] Xavier Taixes i Ventosa and Gabor Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, arXiv:0909.2724v2 (2009).
- [93] David Jao and Vladimir Soukharev, *A subexponential algorithm for evaluating large degree isogenies*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 6197, Springer, Berlin, 2010, pp. 219–233.
- [94] Jean-François Jaulent, Sebastian Pauli, Michael E. Pohst, and Florence Soriano-Gafiuk, *Computation of 2-groups of positive classes of exceptional number fields*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 715–732. MR MR2523314
- [95] Antoine Joux and Reynald Lercier, *Counting points on elliptic curves in medium characteristic*, 2006, p. 15.
- [96] Ben Kane, *CM liftings of supersingular elliptic curves*, 2009.
- [97] Markus Kirschmer and John Voight, *Algorithmic enumeration of ideal classes for quaternion orders*, SIAM J. Comput **39** (2010), no. 5, 1714–1747.
- [98] Jürgen Klüners, *Algorithms for function fields*, Experiment. Math. **11** (2002), no. 2, 171–181. MR MR1959261 (2003k:11193)
- [99] Alan G.B. Lauder, *Degenerations and limit Frobenius structures in rigid cohomology*, 2009.
- [100] Grégoire Lecerf, *Fast separable factorization and applications*, Appl. Algebra Engrg. Comm. Comput. **19** (2008), no. 2, 135–160. MR MR2389971 (2009b:13069)
- [101] D. Lehavi and C. Ritzenthaler, *An explicit formula for the arithmetic-geometric mean in genus 3*, Experiment. Math. **16** (2007), no. 4, 421–440. MR MR2378484 (2008k:14070)
- [102] Reynald Lercier and Thomas Sirvent, *On Elkies subgroups of  $l$ -torsion points in elliptic curves defined over a finite field*, J. Théor. Nombres Bordeaux **20** (2008), no. 3, 783–797. MR MR2523317

- [103] Rudolf Lidl, *Computational problems in the theory of finite fields*, Appl. Algebra Engrg. Comm. Comput. **2** (1991), no. 2, 81–89. MR MR1325520 (95m:11134)
- [104] J. M. Miret, R. Moreno, J. Pujolàs, and A. Rio, *Halving for the 2-Sylow subgroup of genus 2 curves over binary fields*, Finite Fields Appl. **15** (2009), no. 5, 569–579. MR MR2554040
- [105] Marcel Mohyla and Gabor Wiese, *A computational study of the asymptotic behaviour of coefficient fields of modular forms*, 2009.
- [106] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions*.
- [107] I. Morel, D. Stehlé, and G. Villard, *Analyse numerique et reduction de reseaux*, 2009.
- [108] J.-M. Muller, N. Brisebarre, F. de Dinechin, C.-P. Jeannerod, L. Vincent, G. Melquiond, N. Revol, D. Stehlé, and S. Torres, *Handbook of floating-point arithmetic*, Birkhäuser, Boston, MA, 2009.
- [109] Siguna Müller, *On the computation of square roots in finite fields*, Des. Codes Cryptogr. **31** (2004), no. 3, 301–312. MR MR2047886 (2005f:11278)
- [110] Phong Q. Nguên and Damien Stehlé, *Floating-point LLL revisited*, Advances in cryptology—EUROCRYPT 2005, Lecture Notes in Comput. Sci., vol. 3494, Springer, Berlin, 2005, pp. 215–233. MR MR2352190 (2008m:94017)
- [111] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group  $c_2 \times c_2 \times c_2$* , Journal of Number Theory **129** (2009), no. 1, 231 – 245.
- [112] Titus Piezas, *Solving solvable sextics using polynomial decomposition*, 2004.
- [113] M. E. Pohst, *Computational aspects of Kummer theory*, Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 259–272. MR MR1446518 (98f:11112)
- [114] Xavier-François Roblot, *Polynomial factorization algorithms over number fields*, J. Symbolic Comput. **38** (2004), no. 5, 1429–1443. MR MR2168722
- [115] Tanaka Satoru and Nakamura Ken, *More constructing pairing-friendly elliptic curves for cryptography*, 2007.



- [116] René Schoof, *Computing Arakelov class groups*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 447–495. MR MR2467554
- [117] Nigel P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts, vol. 41, Cambridge University Press, Cambridge, 1998. MR MR1689189 (2000c:11208)
- [118] B. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, J. Cryptology **22** (2009), no. 4, 505–529.
- [119] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 163–180.
- [120] Damien Stehlé, *Floating-point LLL: Theoretical and practical aspects*, Proceedings of LLL+25 Conference, 2007 (2009).
- [121] Damien Stehlé, *Floating-point LLL: Theoretical and practical aspects*, Information Security and Cryptography: The LLL Algorithm (Berlin Heidelberg) (David Basin, Ueli Maurer, Phong Q. Nguyen, and Brigitte Vallée, eds.), Information Security and Cryptography, Springer, 2010, pp. 179–213.
- [122] Damien Stehlé and Paul Zimmermann, *A binary recursive GCD algorithm*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 411–425. MR MR2138011
- [123] William A. Stein, *An introduction to computing modular forms using modular symbols*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 641–652. MR MR2467560 (2009k:11085)
- [124] Katsuyuki Takashima, *A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 124–133.
- [125] Nicolas M. Thiéry, *Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis*, Discrete Mathematics and Theoretical Computer Science: 4th International Conference, DMTCS 2003, Dijon, France, July 7-12, 2003: Proceedings (Berlin) (Cristian Calude, Michael J. Dinneen, and Vincent

- Vajnovszki, eds.), Lecture Notes in Computer Science, vol. 2731, Springer, 2003, pp. 315–328.
- [126] Hans-Christian Graf v. Bothmer, *Finite field experiments (with an appendix by Stefan Wiedmann)*, Higher-Dimensional Geometry over Finite Fields, NATO Science for Peace and Security Series, D: Information and Communication Security, vol. 16, IOS Press, 2008, pp. 1–62.
- [127] Mark van Hoeij, *Factoring polynomials and the knapsack problem*, J. Number Theory **95** (2002), no. 2, 167–189. MR MR1924096 (2003f:13029)
- [128] Gilles Villard, *Certification of the QR factor R and of lattice basis reducedness*, IS-SAC 2007, ACM, New York, 2007, pp. 361–368. MR MR2402283
- [129] P. G. Walsh, *On a very particular class of Ramanujan-Nagell type equations*, Far East J. Math. Sci. (FJMS) **24** (2007), no. 1, 55–58. MR MR2281854 (2007k:11213)
- [130] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.
- [131] Paul Zimmermann and Bruce Dodson, *20 years of ECM*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 525–542. MR MR2282947

# Numerical Analysis

## All Areas

65Xxx

- [1] Tobias Beck and Josef Schicho, *Curve parametrization over optimal field extensions exploiting the Newton polygon*, Geometric Modeling and Algebraic Geometry, Springer, Berlin, 2008, pp. 119–140. MR MR2381607 (2009b:65032)
- [2] Laurent Fousse, Guillaume Hanrot, Vincent Lefèvre, Patrick Pélicier, and Paul Zimmermann, *MPFR: a multiple-precision binary floating-point library with correct rounding*, ACM Trans. Math. Software **33** (2007), no. 2, Art. 13, 15. MR MR2326955
- [3] Shuhong Gao, Guangran Jiang, and Mingfu Zhu, *Solving the 100 Swiss Francs problem*, 2008.
- [4] Vladimir P. Gerdt, Yuri A. Blinkov, and Vladimir V. Mozhilkin, *Gröbner bases and generation of difference schemes for partial differential equations*, SIGMA Symmetry Integrability Geom. Methods Appl. **2** (2006), Paper 051, 26 pp. (electronic). MR MR2240724
- [5] Marc Giusti and Éric Schost, *Solving some overdetermined polynomial systems*, ISSAC '99: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC) (New York), ACM, 1999, pp. 1–8 (electronic). MR MR1802060 (2002b:65084)
- [6] Peter Kirrinnis, *Partial fraction decomposition in  $C(z)$  and simultaneous Newton iteration for factorization in  $C[z]$* , J. Complexity **14** (1998), no. 3, 378–444. MR MR1646107 (2000e:65052)
- [7] Greg Kuperberg, *Numerical cubature from Archimedes' hat-box theorem*, SIAM J. Numer. Anal. **44** (2006), no. 3, 908–935 (electronic). MR MR2231849
- [8] ———, *Numerical cubature using error-correcting codes*, SIAM J. Numer. Anal. **44** (2006), no. 3, 897–907 (electronic). MR MR2231848

# Probability and Statistics

## Probability

60Xxx

- [1] László Babai and Igor Pak, *Strong bias of group generators: An obstacle to the “product replacement algorithm”*, J. Algorithms **50** (2004), no. 2, 215–231, SODA 2000 special issue. MR MR2053017 (2005b:60012)
- [2] Alexandre V. Borovik, *Centralisers of involutions in black box groups*, Computational and Statistical Group Theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 7–20. MR MR1929713 (2003i:60010)
- [3] Weronika Buczyńska, *Phylogenetic varieties on graphs*, 2010.
- [4] Robin Christian, Marston Conder, and Arkadii Slinko, *Flippable pairs and subset comparisons in comparative probability orderings*, Order **24** (2007), no. 3, 193–213. MR MR2358081 (2008j:60048)
- [5] Marston Conder and Arkadii Slinko, *A counterexample to Fishburn’s conjecture on finite linear qualitative probability*, J. Math. Psych. **48** (2004), no. 6, 425–431. MR MR2108382 (2006c:60006)
- [6] P. Diaconis and L. Saloff-Coste, *Walks on generating sets of groups*, Invent. Math. **134** (1998), no. 2, 251–299. MR MR1650316 (2000e:60013)
- [7] Persi Diaconis, *The Markov chain Monte Carlo revolution*, Bull. Amer. Math. Soc. (N.S.) **46** (2009), no. 2, 179–205. MR MR2476411
- [8] Jason Fulman, *Random matrix theory over finite fields*, Bull. Amer. Math. Soc. (N.S.) **39** (2002), no. 1, 51–85 (electronic). MR MR1864086 (2002i:60012)
- [9] C. R. Leedham-Green and Scott H. Murray, *Variants of product replacement*, Computational and Statistical Group Theory (Las Vegas, NV/Hoboken, NJ, 2001), Contemp. Math., vol. 298, Amer. Math. Soc., Providence, RI, 2002, pp. 97–104. MR MR1929718 (2003h:20003)

- [10] Alexander Lubotzky and Igor Pak, *The product replacement algorithm and Kazhdan's property (T)*, J. Amer. Math. Soc. **14** (2001), no. 2, 347–363 (electronic). MR1815215 (2003d:60012)

# Statistics

62Xxx

- [1] Joel E. Atkins and Gary J. Sherman, *Sets of typical subsamples*, *Statist. Probab. Lett.* **14** (1992), no. 2, 115–117. MR MR1173408 (93e:62008)
- [2] R. A. Bailey, *Strata for randomized experiments*, *J. Roy. Statist. Soc. Ser. B* **53** (1991), no. 1, 27–78, With discussion and a reply by the author. MR MR1094275 (92k:62134)
- [3] H. Evangelaras, I. Kotsireas, and C. Koukouvinos, *Application of Gröbner bases to the analysis of certain two or three level factorial designs*, *Adv. Appl. Stat.* **3** (2003), no. 1, 1–13. MR MR1983030 (2004d:62268)
- [4] H. Evangelaras and C. Koukouvinos, *Combined arrays with minimum number of runs and maximum estimation efficiency*, *Comm. Statist. Theory Methods* **33** (2004), no. 7, 1621–1628. MR MR2066372
- [5] Shuhong Gao, Guangran Jiang, and Mingfu Zhu, *Solving the 100 Swiss Francs problem*, 2008.
- [6] S. Georgiou and C. Koukouvinos, *Some results on orthogonal designs and Hadamard matrices*, *Int. J. Appl. Math.* **17** (2005), no. 4, 433–443. MR MR2199768 (2007b:05032)
- [7] S. Georgiou, C. Koukouvinos, and S. Stylianou, *Construction of new skew Hadamard matrices and their use in screening experiments*, *Comput. Statist. Data Anal.* **45** (2004), no. 3, 423–429. MR MR2050247
- [8] Alexey Koloydenko, *Symmetric measures via moments*, *Bernoulli* **14** (2008), no. 2, 362–390.
- [9] E. M. Rains, N. J. A. Sloane, and John Stufken, *The lattice of  $N$ -run orthogonal arrays*, *J. Statist. Plann. Inference* **102** (2002), no. 2, 477–500, Silver jubilee issue. MR MR1897221 (2003c:62138)

# Topological and Lie Groups

## Lie Groups

22Exx

- [1] Donald I. Cartwright and Tim Steger, *Application of the Bruhat–Tits tree of  $SU_3(h)$  to some  $A_2$  groups*, J. Austral. Math. Soc. Ser. A **64** (1998), no. 3, 329–344. MR MR1623286 (99i:11026)
- [2] Bruce W. Westbury, *Invariant tensors and the cyclic sieving phenomenon*, 2010.
- [3] Gabor Wiese, *On modular symbols and the cohomology of Hecke triangle surfaces*, Int. J. Number Theory **5** (2009), no. 1, 89–108. MR MR2499023
- [4] Clarence W. Wilkerson, Jr., *Lab notes on the exceptional Lie group  $E_8$  at the prime 2*, 2005.

# Noncompact Transformation Groups

22Fxx

- [1] Daniel Goldstein and Robert Guralnick, *Alternating forms and self-adjoint operators*, J. Algebra **308** (2007), no. 1, 330–349. MR MR2290925



# Topology

## General Topology

54Xxx

- [1] H. O. Erdin, *Pattern equivariant representation variety of tiling spaces for any group  $G$* , 2010.
- [2] P. Christopher Staecker, *Computing twisted conjugacy classes in free groups using nilpotent quotients*, 2007.
- [3] ———, *Remnant properties in nielsen coincidence theory*, 2008.

# Algebraic Topology

55Xxx, 55Rxx, 55Sxx

- [1] K. K. S. Andersen, J. Grodal, J. M. Møller, and A. Viruel, *The classification of  $p$ -compact groups for  $p$  odd*, Ann. of Math. (2) **167** (2008), no. 1, 95–210. MR MR2373153 (2009a:55012)
- [2] Thomas Baird, *GKM sheaves and nonorientable surface group representations*, 2010.
- [3] Dave Benson, *Conway's group  $Co_3$  and the Dickson invariants*, Manuscripta Math. **85** (1994), no. 2, 177–193. MR MR1302871 (95h:55018)
- [4] Carles Broto and Jesper M. Møller, *Embeddings of  $DI_2$  in  $F_4$* , Trans. Amer. Math. Soc. **353** (2001), no. 11, 4461–4479 (electronic). MR MR1851179 (2002e:55015)
- [5] R. F. Brown, M. Furi, L. Górniewicz, and B. Jiang (eds.), *Handbook of Topological Fixed Point Theory*, Springer, Dordrecht, 2005. MR MR2170491 (2006e:55001)
- [6] Robert R. Bruner, Lê M. Hà, and Nguyễn H. V. Hung, *On the behavior of the algebraic transfer*, Trans. Amer. Math. Soc. **357** (2005), no. 2, 473–487 (electronic). MR MR2095619 (2005k:55010)
- [7] O. Davey, E. Hart, and K. Trapp, *Computation of Nielsen numbers for maps of closed surfaces*, Trans. Amer. Math. Soc. **348** (1996), no. 8, 3245–3266. MR MR1370638 (97g:55001)
- [8] Donald M. Davis, *Homotopy type and  $v_1$ -periodic homotopy groups of  $p$ -compact groups*, Topology and its Applications **156** (2008), no. 2, 300 – 321.
- [9] Evelyn L. Hart and Edward C. Keppelmann, *Explorations in Nielsen periodic point theory for the double torus*, Topology Appl. **95** (1999), no. 1, 1–30. MR MR1691929 (2000c:55003)
- [10] ———, *Nielsen periodic point theory for periodic maps on orientable surfaces*, Topology Appl. **153** (2006), no. 9, 1399–1420. MR MR2211207 (2006m:55007)
- [11] John Martino, Stewart Priddy, and Jason Douma, *On stably decomposing products of classifying spaces*, Math. Z. **235** (2000), no. 3, 435–453. MR MR1800206 (2002b:55029)

- [12] Tran Ngoc Nam, *Transfert algébrique et action du groupe linéaire sur les puissances divisées modulo 2*, Ann. Inst. Fourier (Grenoble) **58** (2008), no. 5, 1785–1837. MR MR2445834 (2009g:55025)
- [13] Agnese Ilaria Telloni, *On the groups of some fibered spaces*, J. Group Theory **To appear** (2009).
- [14] R. M. W. Wood, *Problems in the Steenrod algebra*, Bull. London Math. Soc. **30** (1998), no. 5, 449–517. MR MR1643834 (99h:55028)

# Homology Theory

55Nxx, 55Pxx, 55Qxx

- [1] Dave Benson, *An algebraic model for chains on  $\omega BG_p^\wedge$* , Trans. Amer. Math. Soc. **361** (2009), no. 4, 2225–2242.
- [2] Carles Broto and Jesper M. Møller, *Embeddings of  $DI_2$  in  $F_4$* , Trans. Amer. Math. Soc. **353** (2001), no. 11, 4461–4479 (electronic). MR MR1851179 (2002e:55015)
- [3] Robert R. Bruner, *Some root invariants and Steenrod operations in  $\text{Ext}_A(F_2, F_2)$* , Homotopy Theory via Algebraic Geometry and Group Representations (Evanston, IL, 1997), Contemp. Math., vol. 220, Amer. Math. Soc., Providence, RI, 1998, pp. 27–33. MR MR1642887 (99g:55017)
- [4] Robert R. Bruner, Lê M. Hà, and Nguyễn H. V. Hung, *On the behavior of the algebraic transfer*, Trans. Amer. Math. Soc. **357** (2005), no. 2, 473–487 (electronic). MR MR2095619 (2005k:55010)
- [5] Graham Ellis, *On the computation of certain homotopical-functors*, LMS J. Comput. Math. **1** (1998), 25–41 (electronic). MR MR1635723 (99f:55002)
- [6] ———, *Enumerating prime-power homotopy  $k$ -types*, Math. Z. **232** (1999), no. 1, 63–71. MR MR1714280 (2000j:55013)
- [7] R. Levi and S. Priddy, *On certain homotopy actions of general linear groups on iterated products*, Ann. Inst. Fourier (Grenoble) **51** (2001), no. 6, 1719–1739. MR MR1871287 (2002k:55022)
- [8] Jesper M. Moeller,  *$N$ -determined 2-compact groups*, 2005.
- [9] Jesper M. Møller, *The 2-compact groups in the  $A$ -family are  $N$ -determined*, 1997.
- [10] ———, *Toric morphisms between  $p$ -compact groups*, Cohomological Methods in Homotopy Theory (Bellaterra, 1998), Progr. Math., vol. 196, Birkhäuser, Basel, 2001, pp. 271–306. MR MR1851259 (2002i:55010)
- [11] ———,  *$N$ -determined 2-compact groups. I*, Fund. Math. **195** (2007), no. 1, 11–84. MR MR2314074 (2008m:55013)

- [12] ———, *N-determined 2-compact groups. II*, *Fund. Math.* **196** (2007), no. 1, 1–90. MR MR2338539 (2009a:55007)
- [13] Aleš Vavpetič and Antonio Viruel, *On the homotopy type of the classifying space of the exceptional Lie group  $F_4$* , *Manuscripta Math.* **107** (2002), no. 4, 521–540. MR MR1906774 (2003d:55013)

# Spectral Sequences

55Txx

- [1] Mark Behrens and Gerd Laures,  *$\beta$ -family congruences and the  $f$ -invariant*, 2008.
- [2] Robert R. Bruner, Lê M. Hà, and Nguyễn H. V. Hung, *On the behavior of the algebraic transfer*, Trans. Amer. Math. Soc. **357** (2005), no. 2, 473–487 (electronic). MR2095619 (2005k:55010)

# Low-dimensional Topology

57Mxx

- [1] E. Bujalance, F. J. Cirre, M. D. E. Conder, and B. Szepietowski, *Finite group actions on bordered surfaces of small genus*, J. Pure Appl. Algebra **214** (2010), no. 12, 2165–2185. MR 2660907
- [2] Emilio Bujalance, F. J. Cirre, and Marston Conder, *On full automorphism groups of Riemann surfaces*, J. Symbolic Comput. **24** (1997), 235–265.
- [3] J. S. Calcut, *Torelli Actions and Smooth Structures on 4-manifolds*, Phd Thesis, University of Maryland, 2004, p. 84.
- [4] ———, *Knot theory and the Casson invariant in the Artin presentation theory*, Fundam. Prikl. Mat. **11** (2005), no. 4, 119–126. MR MR2192960 (2006m:57013)
- [5] J. S. Calcut, *Rationality and the tangent function*, 2006.
- [6] J. S. Calcut, *Artin presentations from an algebraic viewpoint*, J. Algebra Appl. **6** (2007), no. 2, 355–367. MR MR2316429 (2008d:20057)
- [7] ———, *Torelli actions and smooth structures on four manifolds*, J. Knot Theory Ramifications **17** (2008), no. 2, 171–190. MR MR2398732 (2009b:57061)
- [8] J. S. Calcut and H. E. Winkelnkemper, *Artin presentations of complex surfaces*, Bol. Soc. Mat. Mexicana (3) **10** (2004), 63–87. MR MR2199340 (2006i:57002)
- [9] Frank Calegari and Nathan M. Dunfield, *Automorphic forms and rational homology 3-spheres*, Geom. Topol. **10** (2006), 295–329 (electronic). MR MR2224458 (2007h:57013)
- [10] Jason Callahan, *Jorgensen number and arithmeticity*, Conform. Geom. Dyn **13** (2009), 160–186.
- [11] Abhijit Champanerkar, Jacob Lewis, Max Lipyanskiy, and Scott Meltzer, *Exceptional regions and associated exceptional hyperbolic 3-manifolds*, Experiment. Math. **16** (2007), no. 1, 107–118, With an appendix by Alan W. Reid. MR MR2312981 (2008c:57030)
- [12] Marston Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 359–370. MR MR1041434 (91d:20032)

- [13] ———, *Regular maps with small parameters*, J. Austral. Math. Soc. Ser. A **57** (1994), no. 1, 103–112. MR MR1279289 (95h:05087)
- [14] Marston Conder, *Combinatorial and computational group-theoretic methods in the study of graphs, maps and polytopes with maximal symmetry*, Jack Koolen and Jin Ho Kwak and Ming-Yao Xu, Eds. Applications of Group Theory to Combinatorics, Taylor & Francis Group, London, 2008, pp. 1–11.
- [15] ———, *Genus spectra for symmetric embeddings of graphs on surfaces*, Electronic Notes in Discrete Mathematics **31** (2008), 27 – 31.
- [16] Marston Conder and Brent Everitt, *Regular maps on non-orientable surfaces*, Geom. Dedicata **56** (1995), no. 2, 209–219. MR MR1338960 (96g:05046)
- [17] Marston Conder and Colin Maclachlan, *Compact hyperbolic 4-manifolds of small volume*, Proc. Amer. Math. Soc. **133** (2005), no. 8, 2469–2476 (electronic). MR MR2138890
- [18] Marston Conder, Colin Maclachlan, Sanja Todorovic Vasiljevic, and Steve Wilson, *Bounds for the number of automorphisms of a compact non-orientable surface*, J. London Math. Soc. (2) **68** (2003), no. 1, 65–82. MR MR1980244 (2004b:57025)
- [19] Marston Conder, Gaven Martin, and Anna Torstensson, *Maximal symmetry groups of hyperbolic 3-manifolds*, New Zealand J. Math. **35** (2006), no. 1, 37–62. MR MR2222175 (2006m:57024)
- [20] Marston Conder and Gaven J. Martin, *Cusps, triangle groups and hyperbolic 3-folds*, J. Austral. Math. Soc. Ser. A **55** (1993), no. 2, 149–182. MR MR1232754 (94e:57018)
- [21] Marston Conder, Primož Potočnik, and Jozef Širáň, *Regular hypermaps over projective linear groups*, J. Aust. Math. Soc. **85** (2008).
- [22] Marston Conder and Steve Wilson, *Inner reflectors and non-orientable regular maps*, Discrete Math. **307** (2007), no. 3-5, 367–372. MR MR2287477
- [23] Marston D. E. Conder, *Regular maps and hypermaps of Euler characteristic  $-1$  to  $-200$* , J. Combin. Theory Ser. B **99** (2009), no. 2, 455–459. MR MR2482963 (2010b:05084)



- [24] M. A. Dabkowska, M. K. Dabkowski, V. S. Harizanov, J. H. Przytycki, and M. A. Veve, *Compactness of the space of left orders*, J. Knot Theory Ramifications **16** (2007), no. 3, 257–266. MR MR2320157 (2008a:57022)
- [25] Mieczysław K. Dąbkowski and Józef H. Przytycki, *Burnside obstructions to the Montesinos-Nakanishi 3-move conjecture*, Geom. Topol. **6** (2002), 355–360 (electronic). MR MR1914572 (2003m:57009)
- [26] ———, *Unexpected connections between Burnside groups and knot theory*, Proc. Natl. Acad. Sci. USA **101** (2004), no. 50, 17357–17360 (electronic). MR MR2110443 (2005m:57007)
- [27] Mohamed El Marraki, Nicolas Hanusse, Jörg Zipperer, and Alexander Zvonkin, *Cacti, braids and complex polynomials*, Sémin. Lothar. Combin. **37** (1996), Art. B37b, 36 pp. (electronic). MR MR1462334 (98j:57003)
- [28] B. Everitt and C. Maclachlan, *Constructing hyperbolic manifolds*, Computational and Geometric Aspects of Modern Algebra (Edinburgh, 1998), London Math. Soc. Lecture Note Ser., vol. 275, Cambridge Univ. Press, Cambridge, 2000, pp. 78–86. MR MR1776768 (2001i:57022)
- [29] Brent Everitt, *3-manifolds from Platonic solids*, Topology Appl. **138** (2004), no. 1-3, 253–263. MR MR2035484 (2004m:57031)
- [30] Yan-Quan Feng, Klavdija Kutnar, Aleksander Malnič, and Dragan Marušič, *On 2-fold covers of graphs*, J. Combin. Theory Ser. B **98** (2008), no. 2, 324–341. MR MR2389602 (2009d:05104)
- [31] Véronique Godin, *The unstable integral homology of the mapping class groups of a surface with boundary*, Math. Ann. **337** (2007), no. 1, 15–60. MR MR2262776
- [32] George Havas and L. G. Kovács, *Distinguishing eleven crossing knots*, Computational group theory (Durham, 1982), Academic Press, London, 1984, pp. 367–373. MR MR760671 (86i:57007)
- [33] Stephen P. Humphries, *Intersection-number operators for curves on discs. II*, Geom. Dedicata **86** (2001), no. 1-3, 153–168. MR MR1856422 (2003f:57034)
- [34] ———, *Finite Hurwitz braid group actions for Artin groups*, Israel J. Math. **143** (2004), 189–222. MR MR2106983 (2005i:20061)

- [35] ———, *Intersection-number operators and Chebyshev polynomials. IV. Non-planar cases*, *Geom. Dedicata* **130** (2007), 25–41. MR MR2365776 (2008i:57019)
- [36] Peter Lorimer, *Four dodecahedral spaces*, *Pacific J. Math.* **156** (1992), no. 2, 329–335. MR MR1186809 (94a:57026)
- [37] ———, *Models for a finite universe*, *Internat. J. Theoret. Phys.* **41** (2002), no. 7, 1201–1274. MR MR1923298 (2003h:57020)
- [38] Melissa L. Macasieb, *Derived arithmetic Fuchsian groups of genus two*, *Experiment. Math.* **17** (2008), no. 3, 347–369. MR MR2455706 (2009i:11135)
- [39] Colin Maclachlan and Alan W. Reid, *The Arithmetic of Hyperbolic 3-manifolds*, *Graduate Texts in Mathematics*, vol. 219, Springer-Verlag, New York, 2003. MR MR1937957 (2004i:57021)
- [40] Saburo Matsumoto and Richard Rannard, *The regular projective solution space of the figure-eight knot complement*, *Experiment. Math.* **9** (2000), no. 2, 221–234. MR MR1780207 (2002i:57025)
- [41] Coy L. May, *Groups of even real genus*, *J. Algebra Appl.* **6** (2007), no. 6, 973–989. MR MR2376795 (2008j:57029)
- [42] Coy L. May and Jay Zimmerman, *The symmetric genus of groups of odd order*, *Houston J. Math.* **34** (2008), no. 2, 319–338. MR MR2417394
- [43] David Penneys, *A cyclic approach to the annular Temperley-Lieb category*, 2009.
- [44] Richard Rannard, *Computing immersed normal surfaces in the figure-eight knot complement*, *Experiment. Math.* **8** (1999), no. 1, 73–84. MR MR1685039 (2000h:57031)
- [45] Stephen Tawn, *A presentation for the pure Hilden group*, 2009.
- [46] H. E. Winkelnkemper, *Artin presentations. I. Gauge theory, 3 + 1 TQFT's and the braid groups*, *J. Knot Theory Ramifications* **11** (2002), no. 2, 223–275. MR MR1895372 (2003b:57045)

# Topological Manifolds

57Nxx

- [1] Nathan M. Dunfield and William P. Thurston, *The virtual Haken conjecture: experiments and examples*, *Geom. Topol.* **7** (2003), 399–441 (electronic). MR MR1988291 (2004i:57024)
- [2] Stephen P. Humphries, *Free products in mapping class groups generated by Dehn twists*, *Glasgow Math. J.* **31** (1989), no. 2, 213–218. MR MR997819 (90e:57024)
- [3] ———, *An action of subgroups of mapping class groups on polynomial algebras*, *Topology Appl.* **154** (2007), no. 6, 1053–1083. MR MR2298622

# Topological Groups

57Sxx

- [1] Alejandro Adem, James F. Davis, and Özgün Ünlü, *Fixity and free group actions on products of spheres*, Comment. Math. Helv. **79** (2004), no. 4, 758–778. MR MR2099121 (2006a:57034)

# Computational Topology

55-04

- [1] Graham Ellis, *On the computation of certain homotopical-functors*, LMS J. Comput. Math. **1** (1998), 25–41 (electronic). MR MR1635723 (99f:55002)

# Coding Theory

## Linear Codes: General

94B05, 94B12, 94B60

- [1] Salah A. Aly, *Asymmetric and symmetric subsystem BCH codes and beyond*, 2008.
- [2] E. F. Assmus, Jr. and J. D. Key, *Designs and codes: an update*, Des. Codes Cryptogr. **9** (1996), no. 1, 7–27, Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994). MR MR1412173 (97m:94021)
- [3] ———, *Polynomial codes and finite geometries*, Handbook of Coding Theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1269–1343. MR MR1667952
- [4] Christine Bachoc, *On harmonic weight enumerators of binary codes*, Des. Codes Cryptogr. **18** (1999), no. 1-3, 11–28, Designs and codes—a memorial tribute to Ed Assmus. MR MR1738653 (2002b:94025)
- [5] ———, *Harmonic weight enumerators of nonbinary codes and MacWilliams identities*, Codes and Association Schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 1–23. MR MR1816384 (2002b:94024)
- [6] Lynn M. Batten, Michelle Davidson, and Leo Storme, *An analysis of Chen’s construction of minimum-distance five codes*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 505–511. MR MR1748985 (2000m:94031)
- [7] Thierry P. Berger, *Goppa and related codes invariant under a prescribed permutation*, IEEE Trans. Inform. Theory **46** (2000), no. 7, 2628–2633. MR MR1806822
- [8] Koichi Betsumiya, T. Aaron Gulliver, and Masaaki Harada, *Binary optimal linear rate 1/2 codes*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Honolulu, HI, 1999), Lecture Notes in Comput. Sci., vol. 1719, Springer, Berlin, 1999, pp. 462–471. MR MR1846520 (2002j:94060)
- [9] Ezio Biglieri, John K. Karlof, and Emanuele Viterbo, *Representing group codes as permutation codes*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 2204–2207. MR MR1720681 (2000g:94058)

- [10] Delphine Boucher and Felix Ulmer, *Coding with skew polynomial rings*, J. Symbolic Comput. **44** (2009), no. 12, 1644–1656. MR MR2553570
- [11] Iliya Bouyukliev and Valentin Bakoev, *A method for efficiently computing the number of codewords of fixed weights in linear codes*, Discrete Appl. Math. **156** (2008), no. 15, 2986–3004. MR MR2457507
- [12] Iliya Bouyukliev, Markus Grassl, and Zlatko Varbanov, *New bounds for  $n_4(k, d)$  and classification of some optimal codes over  $\text{GF}(4)$* , Discrete Math. **281** (2004), no. 1-3, 43–66. MR MR2047756 (2005g:94094)
- [13] Iliya Bouyukliev and Juriaan Simonis, *Some new results for optimal ternary linear codes*, IEEE Trans. Inform. Theory **48** (2002), no. 4, 981–985. MR MR1908461 (2003c:94043)
- [14] Thomas Britz and Keisuke Shiromoto, *Designs from subcode supports of linear codes*, Des. Codes Cryptogr. **46** (2008), no. 2, 175–189. MR MR2368992 (2009a:94040)
- [15] Stanislav Bulygin and Ruud Pellikaan, *Bounded distance decoding of linear error-correcting codes with Gröbner bases*, J. Symb. Comput. **44** (2009), no. 12, 1626–1643.
- [16] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane, *Quantum error correction via codes over  $\text{GF}(4)$* , IEEE Trans. Inform. Theory **44** (1998), no. 4, 1369–1387. MR MR1665774 (99m:94063)
- [17] Lionel Chaussade, Pierre Loidreau, and Felix Ulmer, *Skew codes of prescribed distance or rank*, Des. Codes Cryptogr. **Online first** (2008), 18.
- [18] Anne Desideri Bracco, *Treillis de codes quasi-cycliques*, European J. Combin. **25** (2004), no. 4, 505–516. MR MR2069378 (2005c:94073)
- [19] Cunsheng Ding, David Kohel, and San Ling, *Elementary 2-group character codes*, IEEE Trans. Inform. Theory **46** (2000), no. 1, 280–284. MR MR1743594 (2000j:94030)
- [20] Peng Ding and Jennifer D. Key, *Minimum-weight codewords as generators of generalized Reed-Muller codes*, IEEE Trans. Inform. Theory **46** (2000), no. 6, 2152–2158. MR MR1781373 (2001g:94017)
- [21] ———, *Subcodes of the projective generalized Reed-Muller codes spanned by minimum-weight vectors*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 197–211. MR MR1919877 (2004f:94092)

- [22] Thomas Feulner, *The automorphism groups of linear codes and canonical representatives of their semilinear isometry classes*, Adv. Math. Commun. **3** (2009), no. 4, 363–383. MR MR2559135
- [23] Luís R. A. Finotti, *Minimal degree liftings in characteristic 2*, J. Pure Appl. Algebra **207** (2006), no. 3, 631–673. MR MR2265544 (2007g:11068)
- [24] Philippe Gaborit, *Quadratic double circulant codes over fields*, J. Combin. Theory Ser. A **97** (2002), no. 1, 85–107. MR MR1879128 (2002m:94056)
- [25] Philippe Gaborit, W. Cary Huffman, Jon-Lark Kim, and Vera Pless, *On additive GF(4) codes*, Codes and Association Schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 135–149. MR MR1816395 (2002c:94046)
- [26] Philippe Gaborit and Oliver D. King, *Linear constructions for DNA codes*, Theoret. Comput. Sci. **334** (2005), no. 1-3, 99–113. MR MR2132945 (2006b:94073)
- [27] Philippe Gaborit, Carmen-Simona Nedeloaia, and Alfred Wassermann, *Weight enumerators of duadic and quadratic residue codes*, IEEE International Symposium on Information Theory (ISIT), Chicago, USA, 2004.
- [28] Julia Galstad and Gerald Hoehn, *A new class of codes over  $Z_2 \times Z_2$* , 2010.
- [29] Santos González, Consuelo Martínez, and Alejandro P. Nicolás, *Classic and quantum error correcting codes*, Coding Theory and Applications, Lecture Notes in Computer Science, vol. 5228, Springer, 2008, pp. 56–68.
- [30] Daniel M. Gordon, Victor Miller, and Peter Ostapenko, *Optimal hash functions for approximate closest pairs on the  $n$ -cube*, 2008.
- [31] M. Grassl and G. White, *New good linear codes by special puncturings*, International Symposium on Information Theory, 2004. ISIT 2004 (2004), 454–.
- [32] Fernando Hernando and Diego Ruano, *Sixteen new linear codes with Plotkin sum*, 2008.
- [33] W. Cary Huffman and Vera Pless, *Fundamentals of Error-correcting Codes*, Cambridge University Press, Cambridge, 2003. MR MR1996953 (2004k:94077)



- [34] Paul Hurley and Ted Hurley, *Codes from zero-divisors and units in group rings*, International Journal of Information and Coding Theory **1** (2009), no. 1, 57–87.
- [35] Ted Hurley, *Convolutional codes from units in matrix and group rings*, Int. J. Pure Appl. Math. **50** (2009), no. 3, 431–463. MR MR2490664
- [36] Martin Janošov, Martin Husák, Peter Farkaš, and Ana Garcia Armada, *New [47, 15, 16] linear binary block code*, IEEE Trans. Inform. Theory **54** (2008), no. 1, 423–424. MR MR2446769
- [37] John K. Karlof and Yaw O. Chang, *Optimal permutation codes for the Gaussian channel*, IEEE Trans. Inform. Theory **43** (1997), no. 1, 356–358. MR MR1610104 (98j:94005)
- [38] J. D. Key, *Codes and finite geometries*, Proceedings of the Twenty-ninth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1998), vol. 131, 1998, pp. 85–99. MR MR1676476 (2000a:51011)
- [39] ———, *Some error-correcting codes and their applications*, Applied Mathematical Modeling: A Multidisciplinary Approach, Edited by D. R. Shier and K. T. Wallenius, CRC Press, Boca Raton, FL, 1999.
- [40] J. D. Key, B. Novick, and F. E. Sullivan, *Binary codes of structures dual to unitals*, Proceedings of the Twenty-eighth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1997), vol. 123, 1997, pp. 119–124. MR MR1605081 (99d:94043)
- [41] J. D. Key and P. Seneviratne, *Binary codes from rectangular lattice graphs and permutation decoding*, European J. Combin. **28** (2007), no. 1, 121–126. MR MR2261808 (2007g:94086)
- [42] Dae San Kim, *Codes associated with  $O^+(2n, 2^r)$  and power moments of Kloosterman sums*, 2008.
- [43] ———, *Codes associated with orthogonal groups and power moments of Kloosterman sums*, 2008.
- [44] ———, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums*, 2008.

- [45] Jon-Lark Kim, Keith E. Mellinger, and Vera Pless, *Projections of binary linear codes onto larger fields*, SIAM J. Discrete Math. **16** (2003), no. 4, 591–603 (electronic). MR MR2032082 (2005a:94099)
- [46] Chong Jie Lim, *Consta-abelian polyadic codes*, IEEE Trans. Inform. Theory **51** (2005), no. 6, 2198–2206. MR MR2235293
- [47] San Ling, Chaoping Xing, and Ferruh Özbudak, *An explicit class of codes with good parameters and their duals*, Discrete Appl. Math. **154** (2006), no. 2, 346–356. MR MR2194407 (2006h:94257)
- [48] J. Löfvenberg, *Binary fingerprinting codes*, Des. Codes Cryptogr. **36** (2005), no. 1, 69–81. MR MR2152177
- [49] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco, *Classification of linear codes exploiting an invariant*, Contrib. Discrete Math. **1** (2006), no. 1, 1–7 (electronic). MR MR2212135 (2006k:94162)
- [50] Patric R. J. Östergård, *Classifying subspaces of Hamming spaces*, Des. Codes Cryptogr. **27** (2002), no. 3, 297–305. MR MR1928445 (2003i:94060)
- [51] Kevin T. Phelps, *An enumeration of 1-perfect binary codes*, Australas. J. Combin. **21** (2000), 287–298. MR MR1758278 (2001a:94050)
- [52] Ralph-Hardo Schulz, *Check character systems and anti-symmetric mappings*, Computational Discrete Mathematics, Lecture Notes in Comput. Sci., vol. 2122, Springer, Berlin, 2001, pp. 136–147. MR MR1911586
- [53] Anuradha Sharma, Gurmeet K. Bakshi, and Madhu Raka, *Polyadic codes of prime power length*, Finite Fields Appl. **13** (2007), no. 4, 1071–1085. MR MR2360540
- [54] Derek H. Smith, Niema Aboluion, Roberto Montemanni, and Stephanie Perkins, *Linear and nonlinear constructions of DNA codes with Hamming distance  $d$  and constant GC-content*, Discrete Math. **To appear** (2010).
- [55] C. Tjhai, M. Tomlinson, M. Grassl, R. Horan, M. Ahmed, and M. Ambroze, *New linear codes derived from binary cyclic codes of length 151*, IEE Proceedings: Communications **153** (2006), no. 5, 581–585.

- [56] M. van Dijk, S. Egner, M. Greferath, and A. Wassermann, *On binary linear [160, 80, 24] codes*, IEEE International Symposium on Information Theory (ISIT), Yokohama, 2003.
- [57] M. van Eupen and P. Lisonek, *Classification of some optimal ternary linear codes of small length*, Designs, Codes and Cryptography **10** (1997), 63–84.
- [58] Judy L. Walker, *Constructing critical indecomposable codes*, IEEE Trans. Inform. Theory **47** (2001), no. 5, 1780–1795. MR MR1842518 (2002h:94097)
- [59] Harold N. Ward, *An Introduction to Algebraic Coding Theory*, Coding Theory and Quantum Computing, Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 27–52. MR MR2170798 (2006e:94001)

# Cyclic Codes

94B15

- [1] Taher Abualrub, Ali Ghrayeb, Nuh Aydin, and Irfan Siap, *On the construction of skew quasi-cyclic codes*, IEEE Trans. Inform. Theory **56** (2010), no. 5, 2081–2090.
- [2] Maria Carmen V. Amarra and Fidel R. Nemenzo, *On: “ $(1 - u)$ -cyclic codes over  $F_{p^k} + uF_{p^k}$ ”*, Appl. Math. Lett. **21** (2008), no. 11, 1129–1133. MR MR2459836
- [3] Makoto Araya and Masaaki Harada, *MDS codes over  $F_9$  related to the ternary Golay code*, Discrete Math. **282** (2004), no. 1-3, 233–237. MR MR2059522 (2005b:94059)
- [4] Marc A. Armand, *List decoding of generalized Reed-Solomon codes over commutative rings*, IEEE Trans. Inform. Theory **51** (2005), no. 1, 411–419. MR MR2235785 (2007j:94101)
- [5] T. P. Berger, *Quasi-cyclic Goppa codes*, IEEE International Symposium on Information Theory, ISIT 2000, 2000.
- [6] Grégoire Bommier and Francis Blanchet, *Binary quasi-cyclic Goppa codes*, Des. Codes Cryptogr. **20** (2000), no. 2, 107–124. MR MR1774118 (2002b:94044)
- [7] A. Bonnetcaze and P. Udaya, *Cyclic codes and self-dual codes over  $F_2 + uF_2$* , IEEE Trans. Inform. Theory **45** (1999), no. 4, 1250–1255. MR MR1686262 (2000b:94020)
- [8] Nigel Boston, *The minimum distance of the  $[137, 69]$  binary quadratic residue code*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 282. MR MR1677868 (99k:94052)
- [9] ———, *Bounding minimum distances of cyclic codes using algebraic geometry*, International Workshop on Coding and Cryptography (Paris, 2001), Electron. Notes Discrete Math., vol. 6, Elsevier, Amsterdam, 2001, p. 10 pp. (electronic). MR MR1985260 (2004e:94039)
- [10] Nigel Boston and Gary McGuire, *The weight distributions of cyclic codes with two zeros and zeta functions*, J. Symbolic Comput. **45** (2010), no. 7, 723–733. MR 2645974
- [11] D. Boucher, W. Geiselmann, and F. Ulmer, *Skew-cyclic codes*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389. MR MR2322946

- [12] Anne Desideri Bracco, Ann Marie Natividad, and Patrick Solé, *On quintic quasi-cyclic codes*, Discrete Appl. Math. **156** (2008), no. 18, 3362–3375. MR MR2467310 (2010e:94295)
- [13] Danyo Danev and Jonas Olsson, *On a sequence of cyclic codes with minimum distance six*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 673–674. MR MR1748995 (2001a:94041)
- [14] Rumén Daskalov and Markus Grassl, *New cyclic and quasi-cyclic quaternary linear codes*, Proceedings Fifth International Workshop on Optimal Codes and Related Topics, (OC 2007) Balchik, Bulgaria, June 2007, 2007, pp. 56–61.
- [15] Anne Desideri Bracco, *Treillis de codes quasi-cycliques*, European J. Combin. **25** (2004), no. 4, 505–516. MR MR2069378 (2005c:94073)
- [16] Cunsheng Ding and Tor Helleseth, *Generalized cyclotomic codes of length  $p_1^{e_1} \cdots p_t^{e_t}$* , IEEE Trans. Inform. Theory **45** (1999), no. 2, 467–474. MR MR1677011 (2000a:94018)
- [17] Steven T. Dougherty, Masaaki Harada, and Manabu Oura, *Note on the  $g$ -fold joint weight enumerators of self-dual codes over  $Z_k$* , Appl. Algebra Engrg. Comm. Comput. **11** (2001), no. 6, 437–445. MR MR1831938 (2002e:94126)
- [18] M. Esmaeili and S. Yari, *On complementary-dual quasi-cyclic codes*, Finite Fields Appl. **15** (2009), no. 3, 375–386. MR MR2516431
- [19] Philippe Gaborit, Carmen-Simona Nedeloaia, and Alfred Wassermann, *On the weight enumerators of duadic and quadratic residue codes*, IEEE Trans. Inform. Theory **51** (2005), no. 1, 402–407. MR MR2234603
- [20] Markus Grassl, *On the minimum distance of some quadratic-residue codes*, ISIT 2000. Sorrento, Italy, June 25-30, 2000, 2000, pp. 253–253.
- [21] Markus Grassl, *New binary codes from a chain of cyclic codes*, IEEE Trans. Inform. Theory **47** (2001), no. 3, 1178–1181. MR MR1830062
- [22] Markus Grassl and Greg White, *New codes from chains of quasi-cyclic codes*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.
- [23] T. Aaron Gulliver and Masaaki Harada, *Orthogonal frames in the Leech lattice and a type II code over  $Z_{22}$* , J. Combin. Theory Ser. A **95** (2001), no. 1, 185–188. MR MR1840485 (2002d:94061)

- [24] Cem Güneri and Ferruh Özbudak, *Cyclic codes and reducible additive equations*, IEEE Trans. Inform. Theory **53** (2007), no. 2, 848–853. MR MR2302794
- [25] K. J. Horadam and P. Udaya, *A new class of ternary cocyclic Hadamard codes*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 1, 65–73. MR MR1989636 (2004j:94034)
- [26] Doug Kuhlman, *The minimum distance of the [83, 42] ternary quadratic residue code*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 282. MR MR1675978 (99k:94056)
- [27] San Ling and Patrick Solé, *Duadic codes over  $\mathbf{F}_2 + u\mathbf{F}_2$* , Appl. Algebra Engrg. Comm. Comput. **12** (2001), no. 5, 365–379. MR MR1864608 (2002m:94065)
- [28] ———, *Nonlinear  $p$ -ary sequences*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 2, 117–125. MR MR1995563 (2004g:94040)
- [29] Teo Mora and Massimiliano Sala, *On the Gröbner bases of some symmetric systems and their application to coding theory*, J. Symbolic Comput. **35** (2003), no. 2, 177–194. MR MR1958953 (2004c:94118)
- [30] Carmen-Simona Nedeloaia, *On weight distribution of cyclic self-dual codes*, IEEE International Symposium on Information Theory (ISIT), Lausanne, Switzerland,, 2002.
- [31] Carmen-Simona Nedeloaia, *Weight distributions of cyclic self-dual codes*, IEEE Trans. Inform. Theory **49** (2003), no. 6, 1582–1591. MR MR1984951 (2004f:94111)
- [32] Emmanuela Orsini and Massimiliano Sala, *General error locator polynomials for binary cyclic codes with  $t \leq 2$  and  $n < 63$* , IEEE Trans. Inform. Theory **53** (2007), no. 3, 1095–1107. MR MR2302814 (2008b:94122)
- [33] Massimiliano Sala, *Groebner bases and distance of cyclic codes*, Appl. Algebra Engrg. Comm. Comput. **13** (2002), no. 2, 137–162. MR MR1912893 (2003f:94090)
- [34] ———, *Upper bounds on the dual distance of BCH(255,  $k$ )*, Des. Codes Cryptogr. **30** (2003), no. 2, 159–168. MR MR2007208 (2004h:94059)
- [35] ———, *Gröbner basis techniques to compute weight distributions of shortened cyclic codes*, J. Algebra Appl. **6** (2007), no. 3, 403–414. MR MR2337760 (2008k:94091)
- [36] C. Tjhai and M. Tomlinson, *Results on binary cyclic codes*, Electronics Letters **43** (2007), no. 4, 234–235.

- [37] José Felipe Voloch, *Computing the minimal distance of cyclic codes*, *Comput. Appl. Math.* **24** (2005), no. 3, 393–398. MR MR2240450 (2007b:94307)

## Self-Dual Codes

- [1] Christine Bachoc and Philippe Gaborit, *On extremal additive  $\mathbf{F}_4$  codes of length 10 to 18*, J. Théor. Nombres Bordeaux **12** (2000), no. 2, 255–271, Colloque International de Théorie des Nombres (Talence, 1999). MR MR1823184 (2002b:94056)
- [2] ———, *On extremal additive  $F_4$  codes of length 10 to 18*, International Workshop on Coding and Cryptography (Paris, 2001), Electron. Notes Discrete Math., vol. 6, Elsevier, Amsterdam, 2001, p. 10 pp. (electronic). MR MR1985228 (2004d:94037)
- [3] ———, *Designs and self-dual codes with long shadows*, J. Combin. Theory Ser. A **105** (2004), no. 1, 15–34. MR MR2030137 (2005a:94084)
- [4] Christine Bachoc, T. Aaron Gulliver, and Masaaki Harada, *Isodual codes over  $Z_{2k}$  and isodual lattices*, J. Algebraic Combin. **12** (2000), no. 3, 223–240. MR MR1803233 (2001j:94052)
- [5] Eiichi Bannai, Steven T. Dougherty, Masaaki Harada, and Manabu Oura, *Type II codes, even unimodular lattices, and invariant rings*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1194–1205. MR MR1686252 (2000i:94091)
- [6] Koichi Betsumiya, *Minimum Lee weights of type II codes over  $F2r$* , Discrete Math. **308** (2008), no. 14, 3018–3022. MR MR2413878
- [7] Koichi Betsumiya, T. Aaron Gulliver, and Masaaki Harada, *Extremal self-dual codes over  $F_2 \times F_2$* , Des. Codes Cryptogr. **28** (2003), no. 2, 171–186. MR MR1962804 (2004c:94111)
- [8] Koichi Betsumiya and Masaaki Harada, *Binary optimal odd formally self-dual codes*, Des. Codes Cryptogr. **23** (2001), no. 1, 11–21. MR MR1825025 (2002b:94026)
- [9] ———, *Classification of formally self-dual even codes of lengths up to 16*, Des. Codes Cryptogr. **23** (2001), no. 3, 325–332. MR MR1840914 (2002d:94051)
- [10] ———, *Formally self-dual codes related to Type II codes*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 2, 81–88. MR MR1995560 (2004g:94079)
- [11] A. Bonnecaze, P. Solé, and P. Udaya, *Tricolore 3-designs in type III codes*, Discrete Math. **241** (2001), no. 1-3, 129–138. MR MR1861413 (2002m:05031)



- [12] A. Bonnecaze and P. Udaya, *Cyclic codes and self-dual codes over  $F_2 + uF_2$* , IEEE Trans. Inform. Theory **45** (1999), no. 4, 1250–1255. MR MR1686262 (2000b:94020)
- [13] Alexis Bonnecaze, Anne Desideri Bracco, Steven T. Dougherty, Luz R. Nochefranca, and Patrick Solé, *Cubic self-dual binary codes*, IEEE Trans. Inform. Theory **49** (2003), no. 9, 2253–2259. MR MR2004780 (2004i:94052)
- [14] Alexis Bonnecaze, Bernard Mourrain, and Patrick Solé, *Jacobi polynomials, type II codes, and designs*, Des. Codes Cryptogr. **16** (1999), no. 3, 215–234. MR MR1689581 (2000b:05032)
- [15] Stefka Bouyuklieva and Masaaki Harada, *Extremal self-dual  $[50, 25, 10]$  codes with automorphisms of order 3 and quasi-symmetric  $2$ - $(49, 9, 6)$  designs*, Des. Codes Cryptogr. **28** (2003), no. 2, 163–169. MR MR1962803 (2004b:94083)
- [16] Stefka Bouyuklieva, E. A. O’Brien, and Wolfgang Willems, *The automorphism group of a binary self-dual doubly even  $[72, 36, 16]$  code is solvable*, IEEE Trans. Inform. Theory **52** (2006), no. 9, 4244–4248. MR MR2298550
- [17] A. R. Calderbank and N. J. A. Sloane, *Double circulant codes over  $Z_4$  and even unimodular lattices*, J. Algebraic Combin. **6** (1997), no. 2, 119–131. MR MR1436530 (97k:94078)
- [18] Jean-Claude Carlach and Ayoub Otmani, *A systematic construction of self-dual codes*, IEEE Trans. Inform. Theory **49** (2003), no. 11, 3005–3009. MR MR2027579 (2004k:94080)
- [19] Robin Chapman, Steven T. Dougherty, Philippe Gaborit, and Patrick Solé, *2-modular lattices from ternary codes*, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 73–85. MR MR1925991 (2004g:94091)
- [20] Naoki Chigira, Masaaki Harada, and Masaaki Kitazume, *Extremal self-dual codes of length  $64$  through neighbors and covering radii*, Des. Codes Cryptogr. **42** (2007), no. 1, 93–101. MR MR2277060 (2007m:94201)
- [21] ———, *Permutation groups and binary self-orthogonal codes*, J. Algebra **309** (2007), no. 2, 610–621. MR MR2303196
- [22] Daniel B. Dalan, *New extremal binary  $[44, 22, 8]$  codes*, IEEE Trans. Inform. Theory **49** (2003), no. 3, 747–748. MR MR1967201 (2004a:94060)

- [23] ———, *New extremal type I codes of lengths 40, 42, and 44*, Des. Codes Cryptogr. **30** (2003), no. 2, 151–157. MR MR2007207 (2004h:94055)
- [24] Lars Eirik Danielsen and Matthew G. Parker, *On the classification of all self-dual additive codes over  $\text{GF}(4)$  of length up to 12*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1351–1367. MR MR2259065 (2007g:94083)
- [25] Radinka Dontcheva and Masaaki Harada, *Some extremal self-dual codes with an automorphism of order 7*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 2, 75–79. MR MR1995559 (2004f:94093)
- [26] Steven T. Dougherty, Philippe Gaborit, Masaaki Harada, and Patrick Solé, *Type II codes over  $\mathbf{F}_2 + u\mathbf{F}_2$* , IEEE Trans. Inform. Theory **45** (1999), no. 1, 32–45. MR MR1677846 (2000h:94053)
- [27] Steven T. Dougherty, T. Aaron Gulliver, and Manabu Oura, *Higher weights and graded rings for binary self-dual codes*, Discrete Appl. Math. **128** (2003), no. 1, 121–143, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991421 (2004f:94094)
- [28] Steven T. Dougherty, Masaaki Harada, and Manabu Oura, *Note on the biweight enumerators of self-dual codes over  $Z_k$* , 2004.
- [29] J. E. Fields, P. Gaborit, W. C. Huffman, and V. Pless, *On the classification of extremal even formally self-dual codes*, Des. Codes Cryptogr. **18** (1999), no. 1-3, 125–148. MR MR1738661 (2002f:94054)
- [30] ———, *On the classification of extremal even formally self-dual codes of lengths 20 and 22*, Discrete Appl. Math. **111** (2001), no. 1-2, 75–86. MR MR1836720 (2002g:94045)
- [31] Philippe Gaborit, *A bound for certain  $s$ -extremal lattices and codes*, Arch. Math. (Basel) **89** (2007), no. 2, 143–151. MR MR2341725
- [32] Philippe Gaborit, Carmen-Simona Nedeloaia, and Alfred Wassermann, *On the weight enumerators of duadic and quadratic residue codes*, IEEE Trans. Inform. Theory **51** (2005), no. 1, 402–407. MR MR2234603
- [33] Philippe Gaborit and Ayoub Otmani, *Experimental constructions of self-dual codes*, Finite Fields Appl. **9** (2003), no. 3, 372–394. MR MR1983055 (2004f:94096)

- [34] M. Grassl and T. A. Gulliver, *On self-dual MDS codes*, IEEE International Symposium on Information Theory, 2008. ISIT 2008 (2008), 1954–1957.
- [35] Markus Grassl and T. Aaron Gulliver, *On circulant self-dual codes over small fields*, Des. Codes Cryptogr. **52** (2009), no. 1, 57–81.
- [36] T. Aaron Gulliver and Masaaki Harada, *Classification of extremal double circulant formally self-dual even codes*, Des. Codes Cryptogr. **11** (1997), no. 1, 25–35. MR MR1436757 (97k:94084)
- [37] ———, *Classification of extremal double circulant self-dual codes of lengths 64 to 72*, Des. Codes Cryptogr. **13** (1998), no. 3, 257–269. MR MR1601568 (98i:94045)
- [38] ———, *Double circulant self-dual codes over  $Z_{2k}$* , IEEE Trans. Inform. Theory **44** (1998), no. 7, 3105–3123. MR MR1672103 (99m:94043)
- [39] ———, *Double circulant self-dual codes over  $GF(5)$* , Ars Combin. **56** (2000), 3–13. MR MR1768599
- [40] ———, *Classification of extremal double circulant self-dual codes of lengths 74–88*, Discrete Math. **306** (2006), no. 17, 2064–2072. MR MR2251825 (2007e:94109)
- [41] ———, *On double circulant doubly even self-dual  $[72, 36, 12]$  codes and their neighbors*, Australas. J. Combin. **40** (2008), 137–144. MR MR2381421 (2008k:94082)
- [42] T. Aaron Gulliver, Masaaki Harada, and Jon-Lark Kim, *Construction of new extremal self-dual codes*, Discrete Math. **263** (2003), no. 1-3, 81–91. MR MR1955716 (2003m:94083)
- [43] ———, *Construction of some extremal self-dual codes*, Discrete Math. **264** (2003), 55–73.
- [44] T. Aaron Gulliver, Masaaki Harada, and Hiroki Miyabayashi, *Double circulant and quasi-twisted self-dual codes over  $F_5$  and  $F_7$* , Adv. Math. Commun. **1** (2007), no. 2, 223–238. MR MR2306310 (2008b:94109)
- [45] ———, *Optimal double circulant self-dual codes over  $F_4$ . II*, Australas. J. Combin. **39** (2007), 163–174. MR MR2351197 (2008h:94108)
- [46] T. Aaron Gulliver, Masaaki Harada, Takuji Nishimura, and Patric R. J. Östergård, *Near-extremal formally self-dual even codes of lengths 24 and 32*, Des. Codes Cryptogr. **37** (2005), no. 3, 465–471. MR MR2177646

- [47] T. Aaron Gulliver and Jon-Lark Kim, *Circulant based extremal additive self-dual codes over GF(4)*, IEEE Trans. Inform. Theory **50** (2004), no. 2, 359–366. MR MR2044084 (2005a:94113)
- [48] T. Aaron Gulliver, Jon-Lark Kim, and Yoonjin Lee, *New MDS or near-MDS self-dual codes*, IEEE Trans. Inform. Theory **54** (2008), no. 9, 4354–4360. MR MR2451972
- [49] Annika Günther, *A mass formula for self-dual permutation codes*, Finite Fields Appl. **15** (2009), no. 4, 517–533. MR MR2535593
- [50] Sunghyu Han and Jon-Lark Kim, *On self-dual codes over  $F_5$* , Des. Codes Cryptogr. **48** (2008), no. 1, 43–58. MR MR2395089 (2009a:94043)
- [51] Masaaki Harada, *Construction of an extremal self-dual code of length 62*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1232–1233. MR MR1686258 (2000a:94016)
- [52] ———, *New extremal self-dual codes of lengths 36 and 38*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2541–2543. MR MR1725149
- [53] ———, *An extremal doubly even self-dual code of length 112*, Electron. J. Combin. **15** (2008), no. 1, Note 33, 5. MR MR2438589
- [54] ———, *On the existence of frames of the Niemeier lattices and self-dual codes over  $F_p$* , J. Algebra **321** (2009), no. 8, 2345–2352. MR MR2501524 (2010c:94066)
- [55] Masaaki Harada, W. Holzmann, H. Kharaghani, and M. Khorvash, *Extremal ternary self-dual codes constructed from negacirculant matrices*, Graphs Combin. **23** (2007), no. 4, 401–417. MR MR2328944
- [56] Masaaki Harada and Hadi Kharaghani, *Orthogonal designs and MDS self-dual codes*, Australas. J. Combin. **35** (2006), 57–67. MR MR2239304 (2007h:94077)
- [57] Masaaki Harada, Masaaki Kitazume, Akihiro Munemasa, and Boris Venkov, *On some self-dual codes and unimodular lattices in dimension 48*, European J. Combin. **26** (2005), no. 5, 543–557. MR MR2126638 (2005m:94044)
- [58] Masaaki Harada, Masaaki Kitazume, and Michio Ozeki, *Ternary code construction of unimodular lattices and self-dual codes over  $Z_6$* , J. Algebraic Combin. **16** (2002), no. 2, 209–223. MR MR1943589 (2004b:11099)

- [59] Masaaki Harada and Akihiro Munemasa, *A complete classification of ternary self-dual codes of length 24*, J. Combin. Theory Ser. A **116** (2009), no. 5, 1063–1072. MR MR2522420
- [60] Masaaki Harada, Akihiro Munemasa, and Boris Venkov, *Classification of ternary extremal self-dual codes of length 28*, Math. Comp. **78** (2009), no. 267, 1787–1796. MR MR2501075
- [61] Masaaki Harada and Takuji Nishimura, *An extremal singly even self-dual code of length 88*, Adv. Math. Commun. **1** (2007), no. 2, 261–267. MR MR2306315 (2008b:94110)
- [62] Masaaki Harada, Takuji Nishimura, and Radinka Yorgova, *New extremal self-dual codes of length 66*, Math. Balkanica (N.S.) **21** (2007), no. 1-2, 113–121. MR MR2350723 (2008h:94097)
- [63] Masaaki Harada, Michio Ozeki, and Kenichiro Tanabe, *On the covering radius of ternary extremal self-dual codes*, Des. Codes Cryptogr. **33** (2004), no. 2, 149–158. MR MR2080361 (2005d:94214)
- [64] Hyun Kwang Kim, Dae Kyu Kim, and Jon-Lark Kim, *Type I codes over  $GF(4)$* , Ars Combin. **To appear**.
- [65] Jon-Lark Kim, *New extremal self-dual codes of lengths 36, 38, and 58*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 386–393. MR MR1820382 (2002b:94032)
- [66] ———, *New good Hermitian self-dual codes over  $GF(4)$* , IEEE International Symposium on Information Theory (ISIT), Washington, 2001, p. 177.
- [67] ———, *New self-dual codes over  $GF(4)$  with the highest known minimum weights*, IEEE Trans. Inform. Theory **47** (2001), no. 4, 1575–1580. MR MR1830104 (2002b:94033)
- [68] Jon-Lark Kim and Yoonjin Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A **105** (2004), no. 1, 79–95. MR MR2030141 (2004k:94084)
- [69] C. L. Mallows, V. Pless, and N. J. A. Sloane, *Self-dual codes over  $GF(3)$* , SIAM J. Appl. Math. **31** (1976), no. 4, 649–666. MR MR0441541 (55 #14404)
- [70] C.A. Melchor and P. Gaborit, *On the classification of extremal  $[36, 18, 8]$  binary self-dual codes*, IEEE Trans. Inform. Theory **54** (2008), no. 10, 4743–4750.

- [71] Jamshid Moori and B. G. Rodrigues, *A self-orthogonal doubly even code invariant under  $McL : 2$* , J. Combin. Theory Ser. A **110** (2005), no. 1, 53–69. MR MR2128966 (2006a:05174)
- [72] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane, *Self-dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR MR2209183
- [73] Michio Ozeki, *Jacobi polynomials for singly even self-dual codes and the covering radius problems*, IEEE Trans. Inform. Theory **48** (2002), no. 2, 547–557. MR MR1891267 (2003c:94048)
- [74] B. G. Rodrigues, *Self-orthogonal designs and codes from the symplectic groups  $S_4(3)$  and  $S_4(4)$* , Discrete Math. **308** (2008), no. 10, 1941–1950. MR MR2394462 (2009a:05022)
- [75] Marten van Dijk, Sebastian Egner, Marcus Greferath, and Alfred Wassermann, *On two doubly even self-dual binary codes of length 160 and minimum weight 24*, IEEE Trans. Inform. Theory **51** (2005), no. 1, 408–411. MR MR2235784 (2007m:94202)
- [76] R. Yorgova, *Constructing self-dual codes using an automorphism group*, IEEE Information Theory Workshop, 2006. ITW '06 Chengdu (2006), 11–15.
- [77] Radinka Yorgova and Alfred Wassermann, *Binary self-dual codes with automorphisms of order 23*, Des. Codes Cryptogr. **48** (2008), no. 2, 155–164. MR MR2403446
- [78] Radinka Aleksandrova Yorgova, *On binary self-dual codes with automorphisms*, IEEE Trans. Inform. Theory **54** (2008), no. 7, 3345–3351. MR MR2450792

# Algebraic Geometry Codes

94B27, 94B40

- [1] Daniel Augot and Lancelot Pecquet, *A Hensel lifting to replace factorization in list-decoding of algebraic-geometric and Reed-Solomon codes*, IEEE Trans. Inform. Theory **46** (2000), no. 7, 2605–2614. MR MR1806819 (2001m:94061)
- [2] Peter Beelen, *The order bound for general algebraic geometric codes*, Finite Fields Appl. **13** (2007), no. 3, 665–680. MR MR2332494
- [3] Daniel Bierbrauer, *Codes auf hyperelliptischen und trigonalen kurven*, Ph.D. thesis, Ruprecht-Karls-Universität Heidelberg, July 2006, p. 129.
- [4] Grégoire Bommier and Francis Blanchet, *Binary quasi-cyclic Goppa codes*, Des. Codes Cryptogr. **20** (2000), no. 2, 107–124. MR MR1774118 (2002b:94044)
- [5] Chien-Yu Chen and Iwan M. Duursma, *Geometric Reed-Solomon codes of length 64 and 65 over  $F_8$* , IEEE Trans. Inform. Theory **49** (2003), no. 5, 1351–1353. MR MR1984834
- [6] K. L. Clark and J. D. Key, *Geometric codes over fields of odd prime power order*, Proceedings of the Thirtieth Southeastern International Conference on Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1999), vol. 137, 1999, pp. 177–186. MR MR1744201 (2000k:94053)
- [7] Jennifer A. Davis, *Algebraic geometric codes on anticanonical surfaces*, Ph.D. thesis, University of Nebraska, 2007.
- [8] Cunsheng Ding, David R. Kohel, and San Ling, *Split group codes*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 485–495. MR MR1748983 (2001d:94040)
- [9] Cunsheng Ding, Harald Niederreiter, and Chaoping Xing, *Some new codes from algebraic curves*, IEEE Trans. Inform. Theory **46** (2000), no. 7, 2638–2642. MR MR1806824 (2001j:94048)
- [10] Giorgio Faina and Massimo Giulietti, *Decoding Goppa codes with Magma*, Ars Combin. **61** (2001), 221–232. MR MR1863382
- [11] Majid Farhadi and Marc Perret, *Twisting geometric codes*, Finite Fields Appl. **14** (2008), no. 4, 1091–1100. MR MR2457549

- [12] C. Guneri and F. Ozbudak, *Weil-Serre type bounds for cyclic codes*, IEEE Transactions on Information Theory **54** (2008), no. 12, 5381–5395.
- [13] Cem Güneri, Henning Stichtenoth, and Ihsan Taşkın, *Further improvements on the designed minimum distance of algebraic geometry codes*, J. Pure Appl. Algebra **213** (2009), no. 1, 87–97. MR MR2462987
- [14] Johan P. Hansen, *Toric surfaces and codes, techniques and examples*, 2004.
- [15] Nathan Owen Ilten and Hendrik Süß, *AG codes from polyhedral divisors*, 2008.
- [16] David Joyner, *Toric codes over finite fields*, Appl. Algebra Engrg. Comm. Comput. **15** (2004), no. 1, 63–79. MR MR2142431
- [17] David Joyner and Amy Ksir, *Automorphism groups of some AG codes*, IEEE Trans. Inform. Theory **52** (2006), no. 7, 3325–3329. MR MR2240022 (2007c:94280)
- [18] David Joyner and Salahoddin Shokranian, *Remarks on codes from modular curves: Magma application*, 2004.
- [19] Hans-Joachim Kroll and Rita Vincenti, *PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of  $PG(5, 2)$* , Discrete Math. **308** (2008), no. 2-3, 408–414. MR MR2378042 (2008j:94066)
- [20] Thorsten Lagemann, *Codes und automorphismen optimaler artin-schreier-turme*, Ph.D. thesis, Ruprecht-Karls-Universität Heidelberg, April 2006, p. 92.
- [21] Douglas A. Leonard, *A weighted module view of integral closures of affine domains of type I*, Adv. Math. Commun. **3** (2009), no. 1, 1–11.
- [22] John Little and Hal Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), no. 4, 999–1014 (electronic). MR MR2272243
- [23] John Little and Ryan Schwarz, *On  $m$ -dimensional toric codes*, 2005.
- [24] ———, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 349–367. MR MR2322944
- [25] Benjamin Lundell and Jason McCullough, *A generalized floor bound for the minimum distance of geometric Goppa codes*, J. Pure Appl. Algebra **207** (2006), no. 1, 155–164. MR MR2244388 (2007c:94290)



- [26] Gretchen L. Matthews, *Some computational tools for estimating the parameters of algebraic geometry codes*, Coding Theory and Quantum Computing, Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 19–26. MR MR2170797
- [27] Gretchen L. Matthews and Todd W. Michel, *One-point codes using places of higher degree*, IEEE Trans. Inform. Theory **51** (2005), no. 4, 1590–1593. MR MR2241519 (2007b:94311)
- [28] Gary McGuire and José Felipe Voloch, *Weights in codes and genus 2 curves*, Proc. Amer. Math. Soc. **133** (2005), no. 8, 2429–2437 (electronic). MR MR2138886 (2006b:94070)
- [29] Keith E. Mellinger, *Classes of codes from quadratic surfaces of  $PG(3, q)$* , Contrib. Discrete Math. **2** (2007), no. 1, 35–42 (electronic). MR MR2291882 (2008b:94129)
- [30] G. Nebe, *Kneser-Hecke-operators in coding theory*, Abh. Math. Sem. Univ. Hamburg **76** (2006), 79–90. MR MR2293434 (2007m:11090)
- [31] Diego Ruano, *On the parameters of  $r$ -dimensional toric codes*, Finite Fields Appl. **13** (2007), no. 4, 962–976. MR MR2360532
- [32] John A. Ryan and Kondwani Magamba, *Equivalent irreducible Goppa codes and the precise number of quintic Goppa codes of length 32*, AFRICON 2007 (2007), 1–4.
- [33] Pawel Wocjan, *Brill-Noether algorithm construction of geometric Goppa codes and absolute factorization of polynomials*, Ph.D. thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 1999, p. 108.
- [34] Stephen S.-T. Yau and Huaiqing Zuo, *Notes on classification of toric surface codes of dimension 5*, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 2, 175–185. MR MR2511885
- [35] Marcos Zarzar, *Error-correcting codes on low rank surfaces*, Finite Fields Appl. **13** (2007), no. 4, 727–737. MR MR2359313

# Combinatorial Codes

94B25

- [1] Makoto Araya, Masaaki Harada, and Hadi Kharaghani, *Some Hadamard matrices of order 32 and their binary codes*, J. Combin. Des. **12** (2004), no. 2, 142–146. MR MR2036652 (2004m:94092)
- [2] E. F. Assmus, Jr., *The coding theory of finite geometries and designs*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Rome, 1988), Lecture Notes in Comput. Sci., vol. 357, Springer, Berlin, 1989, pp. 1–6. MR MR1008488 (90f:51010)
- [3] E. F. Assmus, Jr. and Arthur A. Drisko, *Binary codes of odd-order nets*, Des. Codes Cryptogr. **17** (1999), no. 1-3, 15–36. MR MR1714366 (2000i:94087)
- [4] E. F. Assmus, Jr. and J. D. Key, *Hadamard matrices and their designs: A coding-theoretic approach*, Trans. Amer. Math. Soc. **330** (1992), no. 1, 269–293. MR MR1055565 (92f:05024)
- [5] ———, *Designs and codes: an update*, Des. Codes Cryptogr. **9** (1996), no. 1, 7–27, Second Upper Michigan Combinatorics Workshop on Designs, Codes and Geometries (Houghton, MI, 1994). MR MR1412173 (97m:94021)
- [6] ———, *Polynomial codes and finite geometries*, Handbook of Coding Theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1269–1343. MR MR1667952
- [7] Robert F. Bailey and John N. Bray, *Decoding the Mathieu group  $M_{12}$* , Adv. Math. Commun. **1** (2007), no. 4, 477–487. MR MR2354049
- [8] R. D. Baker and K. L. Wantz, *Unitals in the code of the Hughes plane*, J. Combin. Des. **12** (2004), no. 1, 35–38. MR MR2024247 (2004j:94030)
- [9] Koichi Betsumiya, T. Aaron Gulliver, Masaaki Harada, and Akihiro Munemasa, *On type II codes over  $F_4$* , IEEE Trans. Inform. Theory **47** (2001), no. 6, 2242–2248. MR MR1873199 (2002m:94070)
- [10] Neil J. Calkin, Jennifer D. Key, and Marialuisa J. de Resmini, *Minimum weight and dimension formulas for some geometric codes*, Des. Codes Cryptogr. **17** (1999), no. 1-3, 105–120. MR MR1714374 (2000i:94077)

- [11] L. L. Carpenter and J. D. Key, *Reed-Muller codes and Hadamard designs from ovals*, J. Combin. Math. Combin. Comput. **22** (1996), 79–85. MR MR1418060 (97h:94021)
- [12] Ying Cheng and N. J. A. Sloane, *Codes from symmetry groups, and a  $[32, 17, 8]$  code*, SIAM J. Discrete Math. **2** (1989), no. 1, 28–37. MR MR976785 (90h:93026)
- [13] Naoki Chigira, Masaaki Harada, and Masaaki Kitazume, *Permutation groups and binary self-orthogonal codes*, J. Algebra **309** (2007), no. 2, 610–621. MR MR2303196
- [14] ———, *Some self-dual codes invariant under the Hall-Janko group*, J. Algebra **316** (2007), no. 2, 578–590. MR MR2356845
- [15] K. L. Clark, J. D. Key, and M. J. de Resmini, *Dual codes of translation planes*, European J. Combin. **23** (2002), no. 5, 529–538. MR MR1931937 (2004b:94084)
- [16] Marston Conder and John McKay, *Markings of the Golay code*, New Zealand J. Math. **25** (1996), no. 2, 133–139. MR MR1421485 (97g:05040)
- [17] A. Cossidente and A. Sonnino, *A geometric construction of a  $[110, 5, 90]_9$ -linear code admitting the Mathieu group  $M_{11}$* , IEEE Trans. Inform. Theory **54** (2008), no. 11, 5251–5252.
- [18] Antonio Cossidente and Alessandro Siciliano, *A geometric construction of an optimal  $[67, 9, 30]$  binary code*, IEEE Trans. Inform. Theory **47** (2001), no. 3, 1187–1189. MR MR1830064 (2002a:94041)
- [19] M. R. Darafsheh, A. Iranmanesh, and R. Kahkeshani, *Some designs and codes invariant under the groups  $S_9$  and  $A_8$* , Des. Codes Cryptogr. **51** (2009), no. 2, 211–223. MR MR2480700 (2009k:05193)
- [20] Steven T. Dougherty, Jon-Lark Kim, and Patrick Solé, *Double circulant codes from two class association schemes*, Adv. Math. Commun. **1** (2007), no. 1, 45–64. MR MR2262767
- [21] Sean V. Droms, Keith E. Mellinger, and Chris Meyer, *LDPC codes generated by conics in the classical projective plane*, Des. Codes Cryptogr. **40** (2006), no. 3, 343–356. MR MR2251325 (2007f:51021)
- [22] D.G. Farmer and K.J. Horadam, *Presemifield bundles over  $GF(p^3)$* , IEEE International Symposium on Information Theory, 2008. ISIT 2008 (2008), 2613–2616.

- [23] W. Fish, J. D. Key, and E. Mwambene, *Graphs, designs and codes related to the  $n$ -cube*, Discrete Math. **309** (2009), no. 10, 3255–3269. MR MR2526744
- [24] ———, *Binary codes from the line graph of the  $n$ -cube*, J. Symbolic Comput. **45** (2010), no. 7, 800–812. MR 2645979
- [25] ———, *Codes from incidence matrices and line graphs of Hamming graphs*, Discrete Math. **310** (2010), no. 13-14, 1884–1897. MR 2629907
- [26] S. Gao and J. D. Key, *Bases of minimum-weight vectors for codes from designs*, Finite Fields Appl. **4** (1998), no. 1, 1–15. MR MR1612056 (99k:94057)
- [27] D. Ghinelli, M. J. de Resmini, and J. D. Key, *Minimum words of codes from affine planes*, J. Geom. **91** (2009), no. 1-2, 43–51.
- [28] Markus Grassl and T. Aaron Gulliver, *On circulant self-dual codes over small fields*, Des. Codes Cryptogr. **52** (2009), no. 1, 57–81. MR MR2496246
- [29] Willem H. Haemers, Christopher Parker, Vera Pless, and Vladimir Tonchev, *A design and a code invariant under the simple group  $\text{Co}_3$* , J. Combin. Theory Ser. A **62** (1993), no. 2, 225–233. MR MR1207734 (93m:94039)
- [30] Masaaki Harada, *Self-orthogonal 3-(56, 12, 65) designs and extremal doubly-even self-dual codes of length 56*, Des. Codes Cryptogr. **38** (2006), no. 1, 5–16. MR MR2191121 (2006h:94250)
- [31] Masaaki Harada and Vladimir D. Tonchev, *Self-orthogonal codes from symmetric designs with fixed-point-free automorphisms*, Discrete Math. **264** (2003), no. 1-3, 81–90, The 2000 Com<sup>2</sup>MaC Conference on Association Schemes, Codes and Designs (Pohang). MR MR1972023 (2004f:94099)
- [32] K. J. Horadam and P. Udaya, *A new class of ternary cocyclic Hadamard codes*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 1, 65–73. MR MR1989636 (2004j:94034)
- [33] J. D. Key, *Bases for codes of designs from finite geometries*, Proceedings of the Twenty-fifth Southeastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1994), vol. 102, 1994, pp. 33–44. MR MR1382355 (97c:94018)

- [34] ———, *Some applications of Magma in designs and codes: Oval designs, Hermitian unitals and generalized Reed-Muller codes*, J. Symbolic Comput. **31** (2001), no. 1-2, 37–53, Computational algebra and number theory (Milwaukee, WI, 1996). MR MR1806205 (2002d:94064)
- [35] ———, *Recent developments in permutation decoding*, Not. S. Afr. Math. Soc. **37** (2006), no. 1, 2–13. MR MR2223306
- [36] J. D. Key and M. J. de Resmini, *Small sets of even type and codewords*, J. Geom. **61** (1998), no. 1-2, 83–104. MR MR1603821 (98k:51024)
- [37] ———, *Ternary dual codes of the planes of order nine*, J. Statist. Plann. Inference **95** (2001), no. 1-2, 229–236, Special issue on design combinatorics: in honor of S. S. Shrikhande. MR MR1829111 (2002b:94031)
- [38] J. D. Key, T. P. McDonough, and V. C. Mavron, *Information sets and partial permutation decoding for codes from finite geometries*, Finite Fields Appl. **12** (2006), no. 2, 232–247. MR MR2206400 (2006k:94182)
- [39] ———, *Partial permutation decoding for codes from affine geometry designs*, J. Geom. **88** (2008), no. 1-2, 101–109. MR MR2398478
- [40] J. D. Key and J. Moori, *Some irreducible codes invariant under the Janko group,  $J_1$  or  $J_2$* , 2008.
- [41] J. D. Key, J. Moori, and B. G. Rodrigues, *On some designs and codes from primitive representations of some finite simple groups*, J. Combin. Math. Combin. Comput. **45** (2003), 3–19. MR MR1982631 (2004m:94094)
- [42] ———, *Binary codes from graphs on triples*, Discrete Math. **282** (2004), no. 1-3, 171–182. MR MR2059517 (2005b:94054)
- [43] ———, *Permutation decoding for the binary codes from triangular graphs*, European J. Combin. **25** (2004), no. 1, 113–123. MR MR2031806 (2005c:94086)
- [44] ———, *Some binary codes from symplectic geometry of odd characteristic*, Util. Math. **67** (2005), 121–128. MR MR2137926 (2006e:94072)
- [45] ———, *Partial permutation decoding of some binary codes from graphs on triples*, Ars Combin. **91** (2009), 363–371. MR MR2501975

- [46] ———, *Ternary codes from graphs on triples*, Discrete Math. **309** (2009), no. 14, 4663–4681. MR MR2533126 (2010e:94298)
- [47] J. D. Key, J. Moori, and B. G. Rodrigues, *Codes associated with triangular graphs, and permutation decoding*, 2010.
- [48] J. D. Key and P. Seneviratne, *Permutation decoding for binary codes from lattice graphs*, Discrete Math. **308** (2008), no. 13, 2862–2867. MR MR2413986
- [49] Jon-Lark Kim and Vera Pless, *Designs in additive codes over  $\text{GF}(4)$* , Des. Codes Cryptogr. **30** (2003), no. 2, 187–199. MR MR2007210 (2005b:94067)
- [50] Jon-Lark Kim and Patrick Solé, *Skew Hadamard designs and their codes*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 135–145. MR MR2438446
- [51] Heisook Lee and Yoonjin Lee, *Construction of self-dual codes over finite rings  $Z_{p^m}$* , J. Combin. Theory Ser. A **115** (2008), no. 3, 407–422. MR MR2402602
- [52] Ka Hin Leung and Qing Xiang, *On the dimensions of the binary codes of a class of unitals*, Discrete Math. **309** (2009), no. 3, 570–575. MR MR2499009
- [53] San Ling and Chaoping Xing, *Polyadic codes revisited*, IEEE Trans. Inform. Theory **50** (2004), no. 1, 200–207. MR MR2051429 (2005a:94106)
- [54] Kirsten Mackenzie, *Codes of designs*, Ph.D. thesis, University of Birmingham, 1989.
- [55] Johannes Maks and Juriaan Simonis, *Optimal subcodes of second order Reed-Muller codes and maximal linear spaces of bivectors of maximal rank*, Des. Codes Cryptogr. **21** (2000), no. 1-3, 165–180. MR MR1801197 (2001j:94049)
- [56] Stefano Marcugini, Alfredo Milani, and Fernanda Pambianco, *NMDS codes of maximal length over  $\mathbf{F}_q$ ,  $8 \leq q \leq 11$* , IEEE Trans. Inform. Theory **48** (2002), no. 4, 963–966. MR MR1908457 (2003e:94109)
- [57] ———, *Classification of the  $(n, 3)$ -arcs in  $\text{PG}(2, 7)$* , J. Geom. **80** (2004), no. 1-2, 179–184. MR MR2176579
- [58] Gary McGuire and Harold N. Ward, *A determination of the weight enumerator of the code of the projective plane of order 5*, Note Mat. **18** (1998), no. 1, 71–99 (1999). MR MR1759017 (2001g:94026)

- [59] ———, *The weight enumerator of the code of the projective plane of order 5*, *Geom. Dedicata* **73** (1998), no. 1, 63–77. MR MR1651899 (99j:94068)
- [60] Jamshid Moori and B. G. Rodrigues, *Some designs and codes invariant under the simple group  $\text{Co}_2$* , *J. Algebra* **316** (2007), no. 2, 649–661. MR MR2358607
- [61] Akihiro Munemasa and Vladimir D. Tonchev, *A new quasi-symmetric 2-(56, 16, 6) design obtained from codes*, *Discrete Math.* **284** (2004), no. 1-3, 231–234. MR MR2071915 (2005b:05027)
- [62] Mona B. Musa, *On some double circulant binary extended quadratic residue codes*, *IEEE Trans. Inform. Theory* **54** (2008), no. 2, 898–905. MR MR2444570
- [63] Christopher Parker and Vladimir D. Tonchev, *Linear codes and doubly transitive symmetric designs*, *Linear Algebra Appl.* **226/228** (1995), 237–246. MR MR1344564 (96e:05021)
- [64] M. van Dijk, S. Egner, M. Greferath, and A. Wassermann, *Geometric codes over fields of odd prime power order*, *IEEE International Symposium on Information Theory (ISIT)*, Yokohama, 2003.
- [65] Steven R. Weller and Sarah J. Johnson, *Iterative decoding of codes from oval designs*, *Defence Applications of Signal Processing, 2001 Workshop* (2001), 1–19.

## Codes over Galois Rings

- [1] Nuh Aydin, Tsvetan Asamov, and T. Aaron Gulliver, *Some open problems on quasi-twisted and related code constructions and good quaternary codes*, IEEE International Symposium on Information Theory, 2007. ISIT 2007 (2007), 856–860.
- [2] Christine Bachoc, T. Aaron Gulliver, and Masaaki Harada, *Isodual codes over  $Z_{2k}$  and isodual lattices*, J. Algebraic Combin. **12** (2000), no. 3, 223–240. MR MR1803233 (2001j:94052)
- [3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva,  *$Z_2Z_4$ -linear codes: generator matrices and duality*, Des. Codes Cryptogr. **54** (2010), no. 2, 167–179. MR MR2576874
- [4] Delphine Boucher, Patrick Solé, and Felix Ulmer, *Skew constacyclic codes over Galois rings*, Adv. Math. Commun. **2** (2008), no. 3, 273–292. MR MR2429458
- [5] Eimear Byrne, Marcus Greferath, and Michael E. O’Sullivan, *The linear programming bound for codes over finite Frobenius rings*, Des. Codes Cryptogr. **42** (2007), no. 3, 289–301. MR MR2298938 (2008c:94053)
- [6] A. R. Calderbank and N. J. A. Sloane, *Double circulant codes over  $Z_4$  and even unimodular lattices*, J. Algebraic Combin. **6** (1997), no. 2, 119–131. MR MR1436530 (97k:94078)
- [7] Marcus Greferath and Emanuele Viterbo, *On  $Z_4$ - and  $Z_9$ -linear lifts of the Golay codes*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2524–2527. MR MR1725143 (2000h:94056)
- [8] T. Aaron Gulliver and Masaaki Harada, *Optimal double circulant  $Z_4$ -codes*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 122–128. MR MR1913458 (2003d:94108)
- [9] T. Aaron Gulliver, Patric R. J. Östergård, and Nikolai I. Senkevitch, *Optimal quaternary linear rate-1/2 codes of length  $\leq 18$* , IEEE Trans. Inform. Theory **49** (2003), no. 6, 1540–1543. MR MR1984943 (2004f:94097)



- [10] Masaaki Harada, *Extremal type II  $Z_4$ -codes of lengths 56 and 64*, J. Combin. Theory Ser. A **117** (2010), no. 8, 1285–1288. MR 2677690
- [11] Masaaki Harada and Tsuyoshi Miezaki, *An upper bound on the minimum weight of type  $ii$ -codes*, J Combin. Theory Ser. A **118** (2010), no. 1, 190–196.
- [12] M. Kiermaier and A. Wassermann, *On the minimum Lee distance of quadratic residue codes over  $Z_4$* , IEEE International Symposium on Information Theory, 2008. ISIT 2008. (2008), 2617–2619.
- [13] Jon-Lark Kim and Yoonjin Lee, *Construction of MDS self-dual codes over Galois rings*, Des. Codes Cryptogr. **45** (2007), no. 2, 247–258. MR MR2341887
- [14] J. Pernas, J. Pujol, and M. Villanueva, *Kernel dimension for some families of quaternary Reed-Muller codes*, Information Security, Lecture Notes in Comput. Sci., vol. 5393, Springer, Berlin, 2008, pp. 128–141.
- [15] Patrick Solé and Virgilio Sison, *Bounds on the minimum homogeneous distance of the  $p$ -ary image of linear block codes over the Galois ring  $\text{GR}(p^r, m)$* , IEEE Trans. Inform. Theory **53** (2007), no. 6, 2270–2273. MR MR2321881 (2008a:94173)

# Low-Density Parity Check Codes

- [1] John Brevik and Michael E. O’Sullivan, *The performance of LDPC codes with large girth*, 2005.
- [2] Sean V. Droms, Keith E. Mellinger, and Chris Meyer, *LDPC codes generated by conics in the classical projective plane*, Des. Codes Cryptogr. **40** (2006), no. 3, 343–356. MR MR2251325 (2007f:51021)
- [3] M. Greferath, M. O’Sullivan, and R. Smarandache, *Construction of good LDPC codes using dilation matrices*, Proc. IEEE Intern. Symp. on Inform. Theory, 2004.
- [4] Sarah J. Johnson and Steven R. Weller, *High-rate LDPC codes from unital designs*, IEEE Global Telecommunications Conference **4** (2003), no. 5, 2036–2040.
- [5] Christine A. Kelley, Deepak Sridhara, and Joachim Rosenthal, *Tree-based construction of LDPC codes having good pseudocodeword weights*, IEEE Trans. Inform. Theory **53** (2007), no. 4, 1460–1478. MR MR2303014 (2008b:94133)
- [6] Jon-Lark Kim, Uri N. Peled, Irina Perepelitsa, and Vera Pless, *Explicit construction of families of LDPC codes with girth at least six*, Proceedings of the Annual Allerton Conference on Communication, Control and Computing, vol. 40, Part 2, 2002, pp. 1024–1031.
- [7] Jon-Lark Kim, Uri N. Peled, Irina Perepelitsa, Vera Pless, and Shmuel Friedland, *Explicit construction of families of LDPC codes with no 4-cycles*, IEEE Trans. Inform. Theory **50** (2004), no. 10, 2378–2388. MR MR2097054 (2005e:94285)
- [8] Sunghwan Kim, Jong-Seon No, Habong Chung, and Dong-Joon Shin, *Cycle analysis and construction of protographs for QC (LDPC) codes with girth larger than 12*, IEEE International Symposium on Information Theory, 2007. ISIT 2007 (2007), 2256–2260.
- [9] Paul F. Kubwalo and John A. Ryan, *Low density parity check irreducible Goppa codes*, AFRICON 2007 (2007).
- [10] G. Malema, *Constructing quasi-cyclic LDPC codes using a search algorithm*, 2007 IEEE International Symposium on Signal Processing and Information Technology (2007), 956–960.

- [11] Keith E. Mellinger, *LDPC codes from triangle-free line sets*, Des. Codes Cryptogr. **32** (2004), no. 1-3, 341–350. MR MR2072337 (2005b:94056)
- [12] Arvind Sridharan, *Design and analysis of LDPC convolutional codes*, Ph.D. thesis, University of Notre Dame, Indiana, February 2005.
- [13] R. Michael Tanner, Deepak Sridhara, Arvind Sridharan, Thomas E. Fuja, and Daniel J. Costello, Jr., *LDPC block and convolutional codes based on circulant matrices*, IEEE Trans. Inform. Theory **50** (2004), no. 12, 2966–2984. MR MR2103477 (2005g:94108)
- [14] Steven R. Weller and Sarah J. Johnson, *Iterative decoding of codes from oval designs*, Defence Applications of Signal Processing, 2001 Workshop (2001), 1–19.
- [15] Steven R. Weller and Sarah J. Johnson, *Regular low-density parity-check codes from oval designs*, European Transactions on Telecommunications **14** (2003), no. 5, 399–409.

# Lattice Codes

94B10

- [1] T. L. Alderson and Keith E. Mellinger, *2-dimensional optical orthogonal codes from Singer groups*, Discrete Appl. Math. **157** (2009), no. 14, 3008–3019. MR MR2553388
- [2] Masaaki Harada, *On the existence of frames of the Niemeier lattices and self-dual codes over  $F_p$* , J. Algebra **321** (2009), no. 8, 2345–2352. MR MR2501524 (2010c:94066)
- [3] C. Hollanti, J. Lahtonen, and Hsiao feng Lu, *Maximal orders in the design of dense space-time lattice codes*, IEEE Transactions on Information Theory **54** (2008), no. 10, 4493–4510.
- [4] C. Hollanti, J. Lahtonen, K. Ranto, and R. Vehkalahti, *On the densest MIMO lattices from cyclic division algebras*, IEEE Trans. Comp. **55** (2009), no. 8, 3751–3780.
- [5] Camilla Hollanti, Jyrki Lahtonen, Kalle Ranto, and Roope Vehkalahti, *Optimal matrix lattices for MIMO codes from division algebras*, IEEE International Symposium on Information Theory. ISIT 2006, July 2006, pp. 783–787.
- [6] Camilla Hollanti and Hsiao-Feng Lu, *Construction methods for asymmetric multiblock space-time codes*, IEEE Trans. Inform. Theory **55** (2009), no. 3, 1086–1103.
- [7] Camilla Hollanti and Kalle Ranto, *Maximal orders in space-time coding: Construction and decoding*, 2008.
- [8] Camilla J. Hollanti, *Order-theoretic methods for space-time coding: Symmetric and asymmetric designs*, PhD Thesis, Turku Centre for Computer Science, 2008.
- [9] Jyrki Lahtonen and Camilla Hollanti, *A new tool: Constructing STBCs from maximal orders in central simple algebras*, IEEE Information Theory Workshop, Punta del Este, Uruguay, March 13–17, 2006, 2006.
- [10] Roope Vehkalahti, *Class field theoretic methods in the design of lattice signal constellations*, Ph.D. thesis, University of Turku, 2008, p. 101.

# Quantum Error-Correcting Codes

See also Quantum Computation

- [1] Salah A. Aly, Andreas Klappenecker, and Kiran Sarvepalli Pradeep, *Subsystem codes*, IEEE International Symposium on Information Theory, Toronto, Canada, 2008 (ISIT 08), IEEE, New York, 2008, pp. 369–373.
- [2] Thomas Beth, Christopher Charnes, Markus Grassl, Gernot Alber, Aldo Delgado, and Michael Mussinger, *A new class of designs which protect against quantum jumps*, Des. Codes Cryptogr. **29** (2003), no. 1-3, 51–70. MR MR1993156 (2004i:94065)
- [3] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane, *Quantum error correction via codes over  $GF(4)$* , IEEE Trans. Inform. Theory **44** (1998), no. 4, 1369–1387. MR MR1665774 (99m:94063)
- [4] Andrew W. Cross, David P. DiVincenzo, and Barbara M. Terhal, *A comparative code study for quantum fault-tolerance*, 2007.
- [5] G. David Forney, Jr., Markus Grassl, and Saikat Guha, *Convolutional and tail-biting quantum error-correcting codes*, IEEE Trans. Inform. Theory **53** (2007), no. 3, 865–880. MR MR2302801
- [6] David G. Glynn, T. Aaron Gulliver, Johannes G. Maks, and Manish K. Gupta, *The geometry of additive quantum codes*, Springer, 2006.
- [7] M. Grassl, Thomas Beth, and T. Pellizzari, *Codes for the quantum erasure channel*, Phys. Rev. A (3) **56** (1997), no. 1, 33–38. MR MR1459695 (98f:81044)
- [8] M. Grassl, Thomas Beth, and M. Rötteler, *On optimal quantum codes*, International Journal of Quantum Information **2** (2004), no. 1, 55–64.
- [9] Markus Grassl and Thomas Beth, *Quantum BCH codes*, Proceedings X Symposium on Theoretical Electrical Engineering. Magdeburg, Sept. 6–9, 1999, 1999, pp. 207–212.
- [10] Markus Grassl and Martin Rötteler, *Quantum block and convolutional codes from self-orthogonal product codes*, Proceedings 2005 IEEE International Symposium on Information Theory (ISIT 2005), 2005, pp. 1018–1022.

- [11] Markus Grassl and Martin Rötteler, *Quantum convolutional codes: Encoders and structural properties*, Forty-Fourth Annual Allerton Conference, Allerton House, UIUC, Illinois, USA Sept 27-29, 2006, 2006, pp. 510–519.
- [12] Min-Hsiu Hsieh, Igor Devetak, and Todd Brun, *General entanglement-assisted quantum error-correcting codes*, Physical Review A (Atomic, Molecular, and Optical Physics) **76** (2007), no. 6, 062313.
- [13] A. Klappenecker and M. Rötteler, *Remarks on Clifford codes*, Quantum Information and Computation **4** (2004), no. 2, 152–160.
- [14] A. Klappenecker and P. K. Sarvepalli, *Clifford code constructions of operator quantum error-correcting codes*, IEEE Transactions on Information Theory **54** (2008), no. 12, 5760–5765.
- [15] Andreas Klappenecker and Martin Rötteler, *Unitary error bases: Constructions, equivalence, and applications*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Toulouse, 2003), Lecture Notes in Comput. Sci., vol. 2643, Springer, Berlin, 2003, pp. 139–149. MR MR2042421 (2005c:94088)
- [16] ———, *On the structure of nonstabilizer Clifford codes*, Quantum Inf. Comput. **4** (2004), no. 2, 152–160. MR MR2065357 (2005h:94086)
- [17] Annika Niehage, *Quantum Goppa codes over hyperelliptic curves*, Diplomarbeit, Universität Mannheim, 2004.
- [18] Annika Niehage, *Nonbinary quantum Goppa codes exceeding the quantum Gilbert-Varshamov bound*, Quantum Inf. Process. **6** (2007), no. 3, 143–158. MR MR2341674 (2008e:94055)
- [19] Michel Planat, *Entangling gates in even Euclidean lattices such as Leech lattice*, 2010.
- [20] Michel Planat and Philippe Jorrand, *Group theory for quantum gates and quantum coherence*, J. Phys. A **41** (2008), no. 18, 182001, 8. MR MR2453960 (2009i:81023)
- [21] Michel Planat and Maurice R. Kibler, *Unitary reflection groups for quantum fault tolerance*, J. Comput. Theor. Nanosci. **7** (2010), no. 9, 1759–1770.
- [22] M. Rötteler, M. Grassl, and Thomas Beth, *On quantum MDS codes*, IEEE International Symposium on Information Theory – Proceedings, 2004, p. 355.

- [23] Harold N. Ward, *An Introduction to Algebraic Coding Theory*, Coding Theory and Quantum Computing, Contemp. Math., vol. 381, Amer. Math. Soc., Providence, RI, 2005, pp. 27–52. MR MR2170798 (2006e:94001)

## Computational Methods

- [1] Tsvetan Asamov and Nuh Aydin, *A search algorithm for linear codes: Progressive dimension growth*, Des. Codes Cryptogr. **45** (2007), no. 2, 213–217. MR MR2341884
- [2] Cesar A. Garcia-Vazquez and Carlos A. Lopez-Andrade, *D-Heaps as hash tables for vectors over a finite ring*, 2009 WRI World Conference on Computer Science and Information Engineering, WRI World Congress on Computer Science and Information Engineering, vol. 3, IEEE, 2009, pp. 162–166.
- [3] Markus Grassl, *Searching for linear codes with large minimum distance*, Discovering Mathematics with Magma, Algorithms Comput. Math., vol. 19, Springer, Berlin, 2006, pp. 287–313. MR MR2278933 (2007j:94087)
- [4] ———, *Computing extensions of linear codes*, IEEE International Symposium on Information Theory, 2007. ISIT 2007 (2007), 476–480.
- [5] Greg White and Markus Grassl, *A new minimum weight algorithm for additive codes*, Proceedings 2006 IEEE International Symposium on Information Theory (ISIT 2006), Seattle, USA, July 2006, IEEE, 2006, pp. 1119–1123.
- [6] Gregory White, *Enumeration-based Algorithms in Coding Theory*, PhD Thesis, University of Sydney, 2007, p. 330.



# Computer Science

## Computer System Organization

68Mxx

- [1] Michael J. Dinneen, Geoffrey Pritchard, and Mark C. Wilson, *Degree- and time-constrained broadcast networks*, *Networks* **39** (2002), no. 3, 121–129. MR MR1897746 (2003c:68012)
- [2] Willi Geiselmann, Jörn Müller-Quade, and Rainer Steinwandt, *Comment on: “A new representation of elements of finite fields  $\text{GF}(2^m)$  yielding small complexity arithmetic circuits” by G. Drolet*, *IEEE Trans. Comput.* **51** (2002), no. 12, 1460–1461. MR MR2012149
- [3] Willi Geiselmann and Rainer Steinwandt, *Yet another sieving device*, *Topics in Cryptology—CT-RSA 2004*, *Lecture Notes in Comput. Sci.*, vol. 2964, Springer, Berlin, 2004, pp. 278–291. MR MR2092251
- [4] ———, *Non-wafer-scale sieving hardware for the NFS: another attempt to cope with 1024-bit*, *Advances in cryptology—EUROCRYPT 2007*, *Lecture Notes in Comput. Sci.*, vol. 4515, Springer, Berlin, 2007, pp. 466–481. MR MR2449226 (2009h:94125)
- [5] Stephen T. Schibell and Richard M. Stafford, *Processor interconnection networks from Cayley graphs*, *Discrete Appl. Math.* **40** (1992), no. 3, 333–357. MR MR1197007 (94a:68005)
- [6] Lewis Stiller, *Exploiting Symmetry on Parallel Architectures*, Ph.D. thesis, John Hopkins University, 1995.

## Software

68Nxx

- [1] Victor Aladjev, *Computer algebra system Maple: A new software library*, Proceedings of the International Conference held in Melbourne and St. Petersburg, June 2-4, 2003 (Peter M. A. Sloot, David Abramson, Alexander V. Bogdanov, Jack J. Dongarra, Albert Y. Zomaya, and Yuriy E. Gorbachev, eds.), Lecture Notes in Computer Science, vol. 2657, Springer-Verlag, Berlin, 2003, pp. lvi+1095. MR MR2086553 (2005c:00014)
- [2] Joseph L. Awange and Erik W. Grafarend, *Solving Algebraic Computational Problems in Geodesy and Geoinformatics*, Springer-Verlag, Berlin, 2005, The answer to modern challenges. MR MR2139870 (2006b:86022)
- [3] Wieb Bosma and John Cannon (eds.), *Discovering Mathematics with Magma*, Algorithms and Computation in Mathematics, vol. 19, Springer-Verlag, Berlin, 2006, Reducing the abstract to the concrete. MR MR2265375
- [4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
- [5] Gregory Butler and John J. Cannon, *Cayley, Version 4: The user language*, ISSAC '88: Proceedings of the 1988 International Symposium on Symbolic and Algebraic Computation (Berlin), vol. 358, Springer-Verlag, 1988, pp. 456–466.
- [6] John Cannon and Catherine Playoust, *Magma: A new computer algebra system*, Euromath Bull. **2** (1996), no. 1, 113–144. MR MR1413180
- [7] Olga Caprotti, James H. Davenport, Mike Dewar, and Julian Padget, *Mathematics on the (Semantic) NET*, The Semantic Web: Research and Applications, Lecture Notes in Comput. Sci., vol. 3053, 2004, pp. 213–224.
- [8] Martin Clayton, *Computer algebra software*, 1997.
- [9] Gene Cooperman, *Parallel GAP: Mature interactive parallel computing*, Groups and computation, III (Columbus, OH, 1999), Ohio State Univ. Math. Res. Inst. Publ., vol. 8, de Gruyter, Berlin, 2001, pp. 123–138. MR MR1829475 (2002d:20001)

- [10] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörning, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Computational algebra and number theory (London, 1993). MR MR1484479 (99g:11150)
- [11] James H. Davenport, *A small OpenMath type system*, SIGSAM Bull. **34** (2000), no. 2, 16–21.
- [12] James H. Davenport, *Equality in computer algebra and beyond*, J. Symbolic Comput. **34** (2002), no. 4, 259–270. MR MR1946634 (2003m:68188)
- [13] Wolfram Decker, *Some introductory remarks on computer algebra*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 121–142. MR MR1905355
- [14] Ian P. Gent, Warwick Harvey, Tom Kelsey, and Steve Linton, *Generic SBDD using computational group theory*, Principles and Practice of Constraint Programming, CP 2003: 9th International Conference, CP 2003, Kinsale, Ireland, September 29–October 3, 2003, Proceedings, Lecture Notes in Comput. Sci., vol. 2833, Springer, Berlin, 2003, pp. 333–347.
- [15] Florent Hivert and Nicolas M. Thiéry, *MuPAD-Combinat, an open-source package for research in algebraic combinatorics*, Sémin. Lothar. Combin. **51** (2004/05), Art. B51z, 70 pp. (electronic). MR MR2080390 (2005c:05001)
- [16] David Joyner and William Stein, *SAGE: System for algebra and geometry experimentation*, SIGSAM Bull. **39** (2005), no. 2, 61–64.
- [17] Robert H. Lewis and Michael Wester, *Comparison of polynomial-oriented computer algebra systems*, SIGSAM Bull. **33** (1999), no. 4, 5–13.
- [18] J. Neubüser, H. Pahlings, and W. Plesken, *CAS; design and use of a system for the handling of characters of finite groups*, Computational Group Theory (Durham, 1982), Academic Press, London, 1984, pp. 195–247. MR MR760658 (86i:20004)
- [19] Virginia Niculescu, *OOLACA: An object oriented library for abstract and computational algebra*, OOPSLA '04: Companion to the 19th annual ACM SIGPLAN conference on Object-oriented programming systems, languages, and applications (New York, NY, USA), ACM Press, 2004, pp. 160–161.

- [20] Virgile Prevosto and Damien Doligez, *Algorithms and proofs inheritance in the Foc language*, J. Automat. Reason. **29** (2002), no. 3-4, 337–363, Mechanizing and automating mathematics: in honor of N. G. de Bruijn. MR MR1966959 (2004b:68196)
- [21] I. I. Reznikov and V. I. Sushchanskii, *A software system for growth analysis of Mealy automata*, Cybernetics and Systems Analysis **42** (2006), no. 2, 265–276.
- [22] Fritz Schwarz, *ALL TYPES: An algebraic language and type system*, Artificial Intelligence and Symbolic Computation: International Conference AISC'98, Plattsburgh, New York, USA, September 1998. Proceedings, Lecture Notes in Computer Science, vol. 1476, Springer, Berlin, 1998, p. 270.
- [23] Stephen M. Watt, Peter A. Broadbery, Samuel S. Dooley, Pietro Iglio, Scott C. Morrison, Jonathan M. Steinbach, and Robert S. Sutor, *A first report on the A Sharp compiler*, von zur Gathen, Joachim and Giesbrecht, Mark (ed.), ISSAC '94. Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation. Oxford, U.K., July 20–22, 1994. New York, NY: ACM Press, 1994, pp. 25–31.
- [24] André Yamba Yamba, Krister Ahlander, and Malin Ljungberg, *Designing for geometrical symmetry exploitation*, Scientific Programming **14** (2006), no. 2, 61–80.

# Theory of Computing

68Qxx

- [1] M. D. Atkinson, *The complexity of algorithms*, Computing Tomorrow, Cambridge Univ. Press, Cambridge, 1996, pp. 1–20. MR MR1441314
- [2] László Babai and Robert Beals, *A polynomial-time theory of black box groups. I*, Groups St. Andrews 1997 in Bath, I, London Math. Soc. Lecture Note Ser., vol. 260, Cambridge Univ. Press, Cambridge, 1999, pp. 30–64. MR MR1676609 (2000h:20089)
- [3] Bernd Bank, Marc Giusti, Joos Heintz, Mohab Safey El Din, and Eric Schost, *On the geometry of polar varieties*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 1, 33–83. MR 2585564
- [4] Michael J. Beeson, *The mechanization of mathematics*, Alan Turing: Life and Legacy of a Great Thinker, Springer, Berlin, 2004, pp. 77–134. MR MR2172456
- [5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
- [6] Murat Cenk and Ferruh Özbudak, *On multiplication in finite fields*, J. Complexity **26** (2010), no. 2, 172–186.
- [7] James H. Davenport, *Abstract data types in computer algebra*, Mathematical Foundations of Computer Science 2000 (Bratislava), Lecture Notes in Comput. Sci., vol. 1893, Springer, Berlin, 2000, pp. 21–35. MR MR1844731
- [8] C. Dominquez, J. Rubio, and F. Sergeraert, *Modelling inheritance as coercion in the Kenzo system*, Journal of Universal Computer Science **12** (2006), 1701–1730.
- [9] Nicholas James Doye, *Order sorted computer algebra and coercions*, Dissertation, University of Bath, 1997.
- [10] Gabriela Jeronimo, Teresa Krick, Juan Sabia, and Martín Sombra, *The computational complexity of the Chow form*, Found. Comput. Math. **4** (2004), no. 1, 41–117. MR MR2035410 (2005c:14083)
- [11] William M. Kantor, *Sylow’s theorem in polynomial time*, J. Comput. System Sci. **30** (1985), no. 3, 359–394. MR MR805654 (87j:68064)

- [12] Andrei Kelarev, *Graph algebras and automata*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 257, Marcel Dekker Inc., New York, 2003. MR MR2064147 (2005e:68001)
- [13] Eugene M. Luks and Pierre McKenzie, *Parallel algorithms for solvable permutation groups*, J. Comput. System Sci. **37** (1988), no. 1, 39–62, 26th IEEE Conference on Foundations of Computer Science (Portland, OR, 1985). MR MR973656 (90f:68094)
- [14] Masayuki Noro, *Modular dynamic evaluation*, ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, 2006, pp. 262–268.
- [15] I. I. Reznikov and V. I. Sushchanskii, *A software system for growth analysis of Mealy automata*, Cybernetics and Systems Analysis **42** (2006), no. 2, 265–276.
- [16] Fritz Schwarz, *ALL TYPES: An algebraic language and type system*, Artificial Intelligence and Symbolic Computation: International Conference AISC'98, Plattsburgh, New York, USA, September 1998. Proceedings, Lecture Notes in Computer Science, vol. 1476, Springer, Berlin, 1998, p. 270.
- [17] Oliver Wienand, Markus Wedler, Dominik Stoffel, Wolfgang Kunz, and Gert-Martin Greuel, *An algebraic approach for proving data correctness in arithmetic data paths*, Computer Aided Verification, Lecture Notes in Computer Science, vol. 5123, Springer Berlin/Heidelberg, 2008, pp. 473–486.

# Artificial Intelligence

68Txx

- [1] Clemens Ballarin, *Computer algebra and theorem proving*, PhD Thesis, University of Cambridge, 1999.
- [2] Clemens Ballarin, Jacques Calmet, and Peter Kullmann, *Integration of deduction and computation*, 2000.
- [3] Michael J. Beeson, *The mechanization of mathematics*, Alan Turing: Life and Legacy of a Great Thinker, Springer, Berlin, 2004, pp. 77–134. MR MR2172456
- [4] Mireille Boutin and Gregor Kemper, *On reconstructing  $n$ -point configurations from the distribution of distances or areas*, Adv. in Appl. Math. **32** (2004), no. 4, 709–735. MR MR2053842 (2005c:68259)
- [5] ———, *On reconstructing configurations of points in  $P^2$  from a joint distribution of invariants*, Appl. Algebra Engrg. Comm. Comput. **15** (2005), no. 6, 361–391. MR MR2134687 (2006a:13011)
- [6] Arjeh Cohen, Scott H. Murray, Martin Pollet, and Volker Sorge, *Certifying solutions to permutation group problems*, Automated Deduction - CADE-19, Lecture Notes in Computer Science, vol. 2741, Springer Berlin/Heidelberg, 2003, pp. 258–273.
- [7] James H. Davenport, *Equality in computer algebra and beyond*, J. Symbolic Comput. **34** (2002), no. 4, 259–270. MR MR1946634 (2003m:68188)
- [8] Andreas Döring, *Kooperation eines theorembeweislers und eines computeralgebrasystems*, Ph.D. thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 1994, p. 22.
- [9] Andreas Franke and Michael Kohlhase, *System description: Mathweb, an agent-based communication layer for distributed automated theorem proving*, Automated Deduction - Cade-16: Proceedings of the 16th International Conference on Automated Deduction, Trento, Italy, July 1999, Lecture Notes in Computer Science, vol. 1632, Springer, Berlin, Heidelberg, 1999, pp. 243–258.

- [10] Harald Ganzinger (ed.), *Automated deduction—CADE-16*, Lecture Notes in Computer Science, vol. 1632, Berlin, Springer-Verlag, 1999, Lecture Notes in Artificial Intelligence. MR MR1730373 (2000h:68009)
- [11] Karsten Homann, *Symbolisches lösung mathematischer probleme durch kooperation algorithmischer und logischer systeme*, Ph.D. thesis, Fakultät für Informatik der Universität Karlsruhe, 1996, p. 198.
- [12] Karsten Homann and Jacques Calmet, *Combining theorem proving and symbolic mathematical computing*, Selected Papers from the Second International Conference on Integrating Symbolic Mathematical Computation and Artificial Intelligence, Lecture Notes in Comput. Sci., vol. 958, Springer, London, 1994, pp. 18–29.
- [13] Cezary Kaliszyk and Freek Wiedijk, *Certified computer algebra on top of an interactive theorem prover*, Towards Mechanized Mathematical Assistants, Lecture Notes in Computer Science, vol. 4573/2007, Springer Berlin / Heidelberg, 2007, pp. 94–105.
- [14] David Nister, Richard Hartley, and Henrik Stewenius, *Using Galois theory to prove structure from motion algorithms are optimal*, Computer Vision and Pattern Recognition, 2007. CVPR '07, 17-22 June 2007.
- [15] S. Petitjean, *Algebraic geometry and computer vision: Polynomial systems, real and complex roots*, J. Math. Imaging Vision **10** (1999), no. 3, 191–220. MR MR1695944 (2001e:68197)
- [16] Tomaz Pisanski, Marko Boben, and Arjana Zitnik, *Interactive conjecturing with VEGA*, Fajtlowicz, Siemion (ed.) et al., Graphs and Discovery, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 69, American Mathematical Society (AMS), Providence, RI, 2005, pp. 351–364.
- [17] Virgile Prevosto and Damien Doligez, *Algorithms and proofs inheritance in the Foc language*, J. Automat. Reason. **29** (2002), no. 3-4, 337–363, Mechanizing and automating mathematics: in honor of N. G. de Bruijn. MR MR1966959 (2004b:68196)
- [18] Fabrice Rouillier, Mohab Safey El Din, and Éric Schost, *Solving the Birkhoff interpolation problem via the critical point method: An experimental study*, ADG '00: Revised Papers from the Third International Workshop on Automated Deduction in Geometry (Zurich, 2000) (Jürgen Richter-Gebert and Dongming Wang, eds.), Lecture Notes in Computer Science, vol. 2061, Springer-Verlag, Berlin, 2001, Lecture Notes in Artificial Intelligence, pp. viii+325. MR MR1908025 (2003a:68007)



- [19] Lewis Stiller, *Multilinear algebra and chess endgames*, Games of no Chance (Berkeley, CA, 1994), Math. Sci. Res. Inst. Publ., vol. 29, Cambridge Univ. Press, Cambridge, 1996, pp. 151–192. MR MR1427964
- [20] Jürgen Zimmer and Louise A. Dennis, *Inductive theorem proving and computer algebra in the MathWeb Software Bus*, Artificial Intelligence, Automated Reasoning, and Symbolic Computation, Lecture Notes in Comput. Sci., vol. 2385, Springer, Berlin, 2002, pp. 319–331. MR MR2052097

# Computing Methodologies

68Uxx

- [1] David C. Banks and Stephen Linton, *Counting cases in marching cubes: Toward a generic algorithm for producing subtopes*, VIS '03: Proceedings of the 14th IEEE Visualization 2003 (VIS'03) (Washington, DC, USA), IEEE Computer Society, 2003, p. 8.
- [2] Mireille Boutin and Gregor Kemper, *Which point configurations are determined by the distribution of their pairwise distances?*, Internat. J. Comput. Geom. Appl. **17** (2007), no. 1, 31–43. MR MR2296253
- [3] Xin Li, Marc Moreno Maza, and Éric Schost, *On the virtues of generic programming for symbolic computation*, Computational Science - ICCS 2007, Lecture Notes in Computer Science, vol. 4488/2007, Springer Berlin / Heidelberg, 2007, pp. 379–596.
- [4] S. Petitjean, *Algebraic geometry and computer vision: Polynomial systems, real and complex roots*, J. Math. Imaging Vision **10** (1999), no. 3, 191–220. MR MR1695944 (2001e:68197)

# Symbolic and Computational Algebra

68W30

- [1] M. D. Atkinson, *The complexity of algorithms*, Computing Tomorrow, Cambridge Univ. Press, Cambridge, 1996, pp. 1–20. MR MR1441314
- [2] Clemens Ballarin, *Computer algebra and theorem proving*, PhD Thesis, University of Cambridge, 1999.
- [3] Clemens Ballarin, Jacques Calmet, and Peter Kullmann, *Integration of deduction and computation*, 2000.
- [4] Michael J. Beeson, *The mechanization of mathematics*, Alan Turing: Life and Legacy of a Great Thinker, Springer, Berlin, 2004, pp. 77–134. MR MR2172456
- [5] J. Borwein and P. Borwein, *Challenges in mathematical computing*, Computing in Science and Engineering **3** (2001), 48–53.
- [6] Wieb Bosma and John Cannon (eds.), *Discovering Mathematics with Magma*, Algorithms and Computation in Mathematics, vol. 19, Springer-Verlag, Berlin, 2006, Reducing the abstract to the concrete. MR MR2265375
- [7] Bonifacio Castano, Joos Heintzb, Juan Llovet, and Raquel Martinez, *On the data structure straight-line program and its implementation in symbolic computation*, Mathematics and Computers in Simulation **51** (2000), no. 5, 497–528.
- [8] Henri Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR MR1228206 (94i:11105)
- [9] Marston Conder, *Semi-automated theorem proving – the impact of computers on research in pure mathematics*, Proceedings of the First Asian Technology Conference in Mathematics. Singapore, December 1995, 1995, pp. 1–8.
- [10] James H. Davenport, *Abstract data types in computer algebra*, Mathematical Foundations of Computer Science 2000 (Bratislava), Lecture Notes in Comput. Sci., vol. 1893, Springer, Berlin, 2000, pp. 21–35. MR MR1844731
- [11] ———, *Equality in computer algebra and beyond*, J. Symbolic Comput. **34** (2002), no. 4, 259–270. MR MR1946634 (2003m:68188)

- [12] Wolfram Decker, *Some introductory remarks on computer algebra*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 121–142. MR MR1905355
- [13] Derek F. Holt, Bettina Eick, and Eamonn A. O’Brien, *Handbook of Computational Group Theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005. MR MR2129747 (2006f:20001)
- [14] S. Marcugini and F. Pambianco, *Minimal 1-saturating sets in  $PG(2, q)$ ,  $q \leq 16$* , Australas. J. Combin. **28** (2003), 161–169. MR MR1998870 (2004g:51010)
- [15] José M. Martín-García,  *$xPerm$ : Fast index canonicalization for tensor computer algebra*, Comput. Phys. Comm. **179** (2008), no. 8, 597 – 603.
- [16] V. Niculescu and G.S. Moldovan, *Building an object oriented computational algebra system based on design patterns*, SYNASC 2005: Symbolic and Numeric Algorithms for Scientific Computing, 2005, 2005.
- [17] S. Petitjean, *Algebraic geometry and computer vision: Polynomial systems, real and complex roots*, J. Math. Imaging Vision **10** (1999), no. 3, 191–220. MR MR1695944 (2001e:68197)
- [18] Cheryl E. Praeger, *Computers in algebra: New answers, new questions*, J. Korean Math. Soc. **38** (2001), no. 4, 763–780, Mathematics in the new millennium (Seoul, 2000). MR MR1838096 (2002d:20002)
- [19] Katsushi Waki, *An introduction to magma (japanese)*, Noda, Matu-Tarow (ed.). Research on the theory and applications of computer algebra. Proceedings of a symposium held at the Research Institute for Mathematical Sciences, Kyoto University, Kyoto, Japan, November 16–18, 1994., RIMS Kokyuroku, vol. 920, Kyoto University, Kyoto, 1995, pp. 173–179. MR )
- [20] Jian Xu, *MEI - A module system for mechanized mathematics*, Phd, McMasters University, 2008.

# Cryptography

## Cryptography: General

- [1] Alex Biryukov, Praveen Gauravaram, Jian Guo, Dmitry Khovratovich, San Ling, Krystian Matusiewicz, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang, *Cryptanalysis of the LAKE hash family*, Fast Software Encryption, Lecture Notes in Computer Science, vol. 5665, Springer, Berlin, 2009, pp. 156–179.
- [2] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. **14** (2008), no. 3, 703–714. MR MR2435056
- [3] An Braeken, Christopher Wolf, and Bart Preneel, *Classification of highly nonlinear Boolean power functions with a randomised algorithm for checking normality*, 2004.
- [4] Marcus Brinkmann and Gregor Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 273–288. MR MR2438456
- [5] Johannes Buchmann, Carlos Coronado, Martin Dring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt, Ulrich Vollmer, and Ralf-Philipp Weinmann, *Post-quantum signatures*, 2004.
- [6] Kelley Burgin, *The nonexistence of a bijective almost perfect nonlinear function of order 16*, Master’s thesis, Auburn University, Alabama, 2002.
- [7] Denis Charles, Kamal Jain, and Kristin Lauter, *Signatures for network coding*, International Journal of Information and Coding Theory **1** (2009), no. 1, 3–14.
- [8] Mihai Cipu, *Dickson polynomials that are permutations*, Serdica Math. J. **30** (2004), no. 2-3, 177–194. MR MR2098331 (2005g:11244)
- [9] Scott Contini and Igor E. Shparlinski, *On Stern’s attack against secret truncated linear congruential generators*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer Berlin / Heidelberg, 2005, pp. 52–60.
- [10] Scott Contini and Yiqun Lisa Yin, *Improved cryptanalysis of securID*, 2003.
- [11] ———, *Fast software-based attacks on SecurID*, Fast Software Encryption (Berlin), Lecture Notes in Computer Science, vol. 3017, Springer-Verlag, 2004, pp. 454–471.

- [12] Deepak Dalai, *On some necessary conditions of boolean functions to resist algebraic attacks*, Ph D thesis, Indian Statistical Institute, Kolkata, India, 2006.
- [13] Alexander W. Dent and Steven D. Galbraith, *Hidden pairings and trapdoor DDH groups*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2006, p. pp.15.
- [14] Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng, *New differential-algebraic attacks and reparametrization of Rainbow*, Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol. 5037, Springer, 2008, pp. 242–257.
- [15] D.G. Farmer and K.J. Horadam, *Presemifield bundles over  $GF(p^3)$* , IEEE International Symposium on Information Theory, 2008. ISIT 2008 (2008), 2613–2616.
- [16] Steven D. Galbraith, Colm Ó hÉigeartaigh, and Caroline Sheedy, *Simplified pairing computation and security implications*, J. Math. Cryptol. **1** (2007), no. 3, 267–281. MR MR2372156 (2009a:94027)
- [17] Willi Geiselmann and Rainer Steinwandt, *Cryptanalysis of a hash function proposed at ICISC 2006*, Information Security and Cryptology - ICISC 2007, Lecture Notes in Computer Science, vol. 4817/2007, Springer Berlin / Heidelberg, 2007, pp. 1–10.
- [18] Willi Geiselmann, Rainer Steinwandt, and Thomas Beth, *Attacking the affine parts of SFLASH*, Cryptography and Coding, Lecture Notes in Comput. Sci., vol. 2260, Springer, Berlin, 2001, pp. 355–359. MR MR2074529
- [19] ———, *Revealing the affine parts of SFLASHv1, SFLASHv2, and FLASH*, Actas de la VII Reunión Española de Criptología y Seguridad de la Información, vol. 7, 2002, pp. 305–314.
- [20] Markus Grassl and Rainer Steinwandt, *Cryptanalysis of an authentication scheme using truncated polynomials*, 2008.
- [21] K. J. Horadam and D. G. Farmer, *Bundles, presemifields and nonlinear functions*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 79–94. MR MR2438442
- [22] Georg Illies and Marian Margraf, *Attacks on the ESA-PSS-04-151 MAC scheme*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 296–310.

- [23] Mariusz Jakubowski, Prasad Naldurg, Vijay Patankar, and Ramarathnam Venkatesan, *Software integrity checking expressions (ICEs) for robust tamper detection*, Information Hiding, Lecture Notes in Computer Science, vol. 4567, 2008, pp. 96–111.
- [24] Gohar M. Kyureghyan and Alexander Pott, *On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences*, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 149–164. MR MR1993164 (2004g:94036)
- [25] P. Loidreau and V. Shorin, *Application of Gröbner bases techniques for searching new sequences with good periodic correlation properties*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.
- [26] Bart Preneel (ed.), *Advances in Cryptology—Eurocrypt 2000*, Lecture Notes in Computer Science, vol. 1807, Berlin, Springer-Verlag, 2000. MR MR1772020 (2001b:94028)
- [27] N. P. Smart, *Attacks on asymmetric cryptosystems: An analysis of Goubin’s refined power analysis attack*, Cryptographic Hardware and Embedded Systems, Lecture Notes in Comput. Sci., vol. 2779, Springer, Berlin, 2003, pp. 281–290.
- [28] Rainer Steinwandt, Markus Grassl, Willi Geiselmann, and Thomas Beth, *Weakness in the  $SL_2(F_{2^n})$  hashing scheme*, Advances in Cryptology—CRYPTO 2000 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1880, Springer, Berlin, 2000, pp. 287–299. MR MR1850050 (2002i:94053)

## Block Ciphers

- [1] Martin Albrecht, *Algebraic attacks on the Courtois Toy cipher*, *Cryptologia* **32** (2008), no. 3, 220–276.
- [2] Martin Albrecht and Carlos Cid, *Algebraic techniques in differential cryptanalysis*, *Fast Software Encryption* (Orr Dunkelman, ed.), *Lecture Notes in Computer Science*, vol. 5665, Springer, 2009, pp. 193–208.
- [3] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, *Cryptographic Hardware and Embedded Systems - CHES 2007*, *Lecture Notes in Computer Science*, vol. 4727/2007, Springer Berlin / Heidelberg, 2007, pp. 450–466.
- [4] Andrey Bogdanov and Andrey Pyshkin, *Algebraic side-channel collision attacks on AES*, 2007.
- [5] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann, *Block ciphers sensitive to Gröbner basis attacks*, *Topics in Cryptology—CT-RSA 2006*, *Lecture Notes in Comput. Sci.*, vol. 3860, Springer, Berlin, 2006, pp. 313–331. MR MR2243996 (2007e:94052)
- [6] Stanislav Bulygin and Michael Brickenstein, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, 2008.
- [7] ———, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, *Math. Comput. Sci.* **3** (2010), no. 2, 185–200.
- [8] Chris Charnes, Martin Rötteler, and Thomas Beth, *On homogeneous bent functions*, *Applied Algebra, Algebraic Algorithms and Error-correcting Codes* (Melbourne, 2001), *Lecture Notes in Comput. Sci.*, vol. 2227, Springer, Berlin, 2001, pp. 249–259. MR MR1913471 (2003e:94065)
- [9] ———, *Homogeneous bent functions, invariants, and designs*, *Des. Codes Cryptogr.* **26** (2002), no. 1-3, 139–154. MR MR1919874 (2003h:05043)
- [10] C. Cid, S. Murphy, and M. Robshaw, *Computational and algebraic aspects of the advanced encryption standard*, *Seventh International Workshop on Computer Algebra in Scientific Computing, CASC 2004*, St. Petersburg, Russia, 2004, pp. 93–103.



- [11] ———, *Small scale variants of the AES*, LNCS 3557, Eds. Gilbert, H. and Handschuh, H., Springer, 2005, pp. 145–162.
- [12] Carlos Cid, Sean Murphy, and Matthew Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, Springer, New York, 2006. MR MR2250327
- [13] Nicolas T. Courtois and Gregory V. Bard, *Algebraic cryptanalysis of the data encryption standard*, Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887/2007, Springer Berlin / Heidelberg, 2007, pp. 152–169.
- [14] Nicolas T. Courtois, Gregory V. Bard, and David Wagner, *Algebraic and slide attacks on KeeLoq*, 2007.
- [15] Jintai Ding, Bo-Yin Yang, Chen-Mou Cheng, Owen Chen, and Vivien Dubois, *Breaking the symmetry: A way to resist the new differential attack*, 2007.
- [16] Tobias Eibach, Gunnar Völkel, and Enrico Pilz, *Optimising Gröbner bases on Bivium*, Math. Comput. Sci. **3** (2010), no. 2, 159–172.
- [17] Jeremy Erickson, Jintai Ding, and Chris Christensen, *Algebraic cryptanalysis of SMS4: Gröbner basis attack and SAT attack compared*, Information, Security and Cryptology – ICISC 2009 (Donghoon Lee and Seokhie Hong, eds.), Lecture Notes in Computer Science, vol. 5984, Springer Berlin/Heidelberg, 2010, pp. 73–86.
- [18] Jean-Charles Faugère and Ludovic Perret, *Algebraic cryptanalysis of Curry and Flurry using correlated messages*, 2008.
- [19] Willi Geiselmann and Rainer Steinwandt, *A short comment on the affine parts of SFLASHv3*, 2003.
- [20] Krystian Matusiewicz, Scott Contini, and Josef Pieprzyk, *Weaknesses of the fork-256 compression function*, 2006, pp. 1–21.
- [21] Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, *A systematic evaluation of compact hardware implementations for the Rijndael S-box*, Topics in Cryptology—CT-RSA 2005, Lecture Notes in Comput. Sci., vol. 3376, Springer, Berlin, 2005, pp. 323–333. MR MR2174386
- [22] Sean Simmons, *Algebraic cryptanalysis of simplified AES\**, Cryptologia **33** (2009), no. 4, 305–314.

## Stream Ciphers

- [1] M. Afzal and A. Masood, *Algebraic cryptanalysis of a NLFSR based stream cipher*, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. (2008), 1–6.
- [2] Mehreen Afzal and Ashraf Masood, *Resistance of stream ciphers to algebraic recovery of internal secret states*, Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT '08 **2** (2008), 625–630.
- [3] Mehreen Afzal, Ashraf Masood, and Naveed Shehzad, *Improved results on algebraic cryptanalysis of A5/2*, Communications in Computer and Information Science **12** (2008), no. 4, 182–189.
- [4] Sultan Zayid Al-Hinai1, Ed Dawson, Matt Henricksen, and Leonie Simpson, *On the security of the LILI family of stream ciphers against algebraic attacks*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 4586/2007, Springer Berlin / Heidelberg, 2007, pp. 11–28.
- [5] Anne Canteaut, *Open problems related to algebraic attacks on stream ciphers*, WCC 2005, Lecture Notes in Comput. Sci., vol. 3969, Springer, Berlin, 2006, pp. 120–134.
- [6] Scott Contini and Igor E. Shparlinski, *On Stern's attack against secret truncated linear congruential generators*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer Berlin / Heidelberg, 2005, pp. 52–60.
- [7] Tobias Eibach, Enrico Pilz, and Gunnar Völkel, *Attacking Bivium using SAT solvers*, Theory and Applications of Satisfiability Testing, SAT 2008, Lecture Notes in Computer Science, vol. 4996, Springer, Berlin, 2008, pp. 63–76.
- [8] Aline Gouget, Hervé Sibert, Come Berbain, Nicolas Courtois, Blandine Debraize, and Chris Mitchell, *Analysis of the bit-search generator and sequence compression techniques*, Fast Software Encryption (Berlin), Lecture Notes in Computer Science, vol. 3557, Springer-Verlag, 2005, pp. 196–214.
- [9] Antoine Joux and Frédéric Muller, *A chosen IV attack against Turing*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 3006, Springer, Berlin, 2004, pp. 194–207. MR MR2094730 (2005f:94106)

- [10] P. Loidreau and V. Shorin, *Application of Gröbner bases techniques for searching new sequences with good periodic correlation properties*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.
- [11] Cameron McDonald, Chris Charnes, and Josef Pieprzyk, *An algebraic analysis of Trivium ciphers based on the boolean satisfiability problem*, 2007.
- [12] Deike Priemuth-Schmid and Alex Biryukov, *Slid pairs in Salsa20 and Trivium*.
- [13] Werner Schindler and Le Van Ly, *How to embed short cycles into large nonlinear feedback-shift registers*, Security in Communications Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers, Lecture Notes in Comput. Sci., vol. 3352, Springer, Berlin, 2005, p. 367.
- [14] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.
- [15] Haina Zhang and Xiaoyun Wang, *Cryptanalysis of stream cipher grain family*, 2009.

# Public Key Cryptography

See also Curve-Based Public Key Cryptography

- [1] Daniel J. Bernstein, *Batch binary edwards*, Advances in Cryptology - CRYPTO 2009, Lecture Notes in Comput. Sci., vol. 5677, Springer, Berlin, 2009, pp. 317–336.
- [2] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret, *Cryptanalysis of the TRMS signature scheme of PKC'05*, Progress in Cryptology, AfricaCrypt 2008, Lecture Notes in Computer Science, vol. 5023, Springer Berlin/Heidelberg, 2008, pp. 143–155.
- [3] Olivier Billet and Gilles Macario-Rat, *Cryptanalysis of the square cryptosystems*, Advances in Cryptology – ASIACRYPT 2009, Lecture Notes in Comput. Sci., vol. 5912, Springer, Berlin, 2009, pp. 451–468.
- [4] Simon R. Blackburn, Carlos Cid, and Steven D. Galbraith, *Cryptanalysis of a cryptosystem based on Drinfeld modules*, 2003.
- [5] Jens-Matthias Bohli, Stefan Röhrich, and Rainer Steinwandt, *Key substitution attacks revisited: Taking into account malicious signers*, 2006, pp. 30–36.
- [6] Jens-Matthias Bohli, Rainer Steinwandt, María Isabel González Vasco, and Consuelo Martínez, *Weak keys in  $MST_1$* , Des. Codes Cryptogr. **37** (2005), no. 3, 509–524. MR MR2177649
- [7] Wieb Bosma, James Hutton, and Eric R. Verheul, *Looking beyond XTR*, Advances in Cryptology—Asiacrypt 2002, Lecture Notes in Comput. Sci., vol. 2501, Springer, Berlin, 2002, pp. 46–63. MR MR2087376 (2006c:94016)
- [8] Charles Bouillaguet, Pierre-Alain Fouque<sup>1</sup>, Antoine Joux, and Joana Treger, *A family of weak keys in HFE (and the corresponding practical key-recovery)*, pp. 1–16.
- [9] An Braeken, Christopher Wolf, and Bart Preneel, *A study of the security of unbalanced oil and vinegar signature schemes*, Topics in Cryptology—CT-RSA 2005, Lecture Notes in Comput. Sci., vol. 3376, Springer, Berlin, 2005, pp. 29–43. MR MR2174368
- [10] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang, *Odd-char multivariate hidden field equations*, 2008.

- [11] Jiun-Ming Chen and Bo-Yin Yang, *Building secure tame-like multivariate public-key cryptosystems: The new TTS*, Information Security and Privacy: 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005. Proceedings, Lecture Notes in Comput. Sci., vol. 3574, Springer, Berlin, 2005, p. 518.
- [12] Robert S. Coulter, George Havas, and Marie Henderson, *Giesbrecht's algorithm, the HFE cryptosystem and Ore's  $p^s$ -polynomials*, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput, vol. 9, World Sci. Publ., River Edge, NJ, 2001, pp. 36–45. MR MR1877440 (2002m:11103)
- [13] J. Ding, J. E. Gower, D. Schmidt, C. Wolf, and Z. Yin, *Complexity estimates for the  $F_4$  attack on the perturbed Matsumoto-Imai cryptosystem*, Cryptography and coding, Lecture Notes in Comput. Sci., vol. 3796, Springer, Berlin, 2005, pp. 262–277. MR MR2235262 (2007f:94036)
- [14] Jintai Ding, Jason E. Gower, and Dieter Schmidt, *Multivariate public key cryptosystems*, Springer, Berlin, 2006.
- [15] Jintai Ding and Dieter Schmidt, *Cryptanalysis of HFEv and internal perturbation of HFE*, Public Key Cryptography—PKC 2005, Lecture Notes in Comput. Sci., vol. 3386, Springer, Berlin, 2005, pp. 288–301. MR MR2174048 (2006j:94061)
- [16] Jintai Ding, Dieter Schmidt, and Fabian Werner, *Algebraic attack on HFE revisited*, Information Security, Lecture Notes in Comput. Sci., vol. 5222, Springer, Berlin, 2008, pp. 215–227.
- [17] Jintai Ding and John Wagner, *Cryptanalysis of rational multivariate public key cryptosystems*, 2007.
- [18] Bettina Eick and Delaram Kahrobaei, *Polycyclic groups: A new platform for cryptology?*, 2004.
- [19] L. Hernandez Encinas, J. Munoz Masque, and A. Queiruga Dios, *Analysis of the efficiency of the Chor–Rivest cryptosystem implementation in a safe-parameter range*, Information Sciences **To appear** (2009).
- [20] Jean-Charles Faugère and Antoine Joux, *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases*, Advances in Cryptology—CRYPTO 2003, Lecture Notes in Comput. Sci., vol. 2729, Springer, Berlin, 2003, pp. 44–60. MR MR2093185 (2005e:94140)

- [21] Patrick Felke, *Computing the uniformity of power mappings: A systematic approach with the multi-variate method over finite fields of odd characteristic*, PhD Thesis, Ruhr Universität Bochum, 2005.
- [22] Michelle Feltz, *On the conjugacy problem in groups and its variants*, Master thesis in mathematics, University of Fribourg, 2010.
- [23] Pierre-Alain Fouque, Gilles Macario-Rat, Ludovic Perret, and Jacques Stern, *Total break of the  $l$ -IC signature scheme*, Public Key Cryptography, PKC 2008, Lecture Notes in Computer Science, vol. 4939, Springer, 2008, pp. 1–17.
- [24] Pierre-Alain Fouque, Gilles Macario-Rat, and Jacques Stern, *Key recovery on hidden monomial multivariate schemes*, Advances in Cryptology, EUROCRYPT 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 19–30.
- [25] Pierrick Gaudry and Éric Schost, *A low-memory parallel version of Matsuo, Chao, and Tsujii's algorithm*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 208–222. MR MR2137355 (2005m:11237)
- [26] Volker Gebhardt, *A new approach to the conjugacy problem in Garside groups*, J. Algebra **292** (2005), no. 1, 282–302. MR MR2166805
- [27] Willi Geiselmann, Willi Meier, and Rainer Steinwandt, *An attack on the isomorphisms of polynomials problem with one secret*, Int. J. Inf. Secur. (2003), no. 2, 59–64.
- [28] Willi Geiselmann and Rainer Steinwandt, *Cryptanalysis of a knapsack-like cryptosystem*, Period. Math. Hungar. **45** (2002), no. 1-2, 35–41. MR MR1955191 (2003m:94062)
- [29] ———, *Yet another sieving device*, Topics in Cryptology—CT-RSA 2004, Lecture Notes in Comput. Sci., vol. 2964, Springer, Berlin, 2004, pp. 278–291. MR MR2092251
- [30] ———, *Non-wafer-scale sieving hardware for the NFS: another attempt to cope with 1024-bit*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 466–481. MR MR2449226 (2009h:94125)
- [31] María Isabel González Vasco, Martin Rötteler, and Rainer Steinwandt, *On minimal length factorizations of finite groups*, Experiment. Math. **12** (2003), no. 1, 1–12. MR MR2002670 (2004h:20035)

- [32] María Isabel González Vasco and Rainer Steinwandt, *Clouds over a public key cryptosystem based on Lyndon words*, Inform. Process. Lett. **80** (2001), no. 5, 239–242. MR MR1864974 (2003h:94037)
- [33] ———, *Obstacles in two public key cryptosystems based on group factorizations*, Tatra Mt. Math. Publ. **25** (2002), 23–37, TATRACRYPT '01 (Liptovský Ján). MR MR1976471 (2004f:94061)
- [34] Markus Grassl, Ivana Ilić, Spyros Magliveras, and Rainer Steinwandt, *Cryptanalysis of the Tillich–Zémor hash function*, J. Cryptology **online first** (2010), 1–9.
- [35] Markus Grassl and Rainer Steinwandt, *Cryptanalysis of an authentication scheme using truncated polynomials*, Inform. Process. Lett. **Article in Press** (2009).
- [36] Anja Groch, Dennis Hofheinz, and Rainer Steinwandt, *A practical attack on the root problem in braid groups*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 121–131. MR MR2389293
- [37] Guillaume Hanrot and Damien Stehlé, *Improved analysis of Kannan’s shortest lattice vector algorithm (extended abstract)*, Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., vol. 4622, Springer, Berlin, 2007, pp. 170–186. MR MR2419600
- [38] Xin Jiang, Jintai Ding, and Lei Hu, *Kipnis-Shamir attack on HFE revisited*, Information Security and Cryptology, Lecture Notes in Computer Science, vol. 4990, Springer Berlin/Heidelberg, 2008, pp. 399–411.
- [39] Ellen Jochemsz and Alexander May, *A polynomial time attack on RSA with private CRT-exponents smaller than  $N^{0.073}$* , Advances in cryptology—CRYPTO 2007, Lecture Notes in Comput. Sci., vol. 4622, Springer, Berlin, 2007, pp. 395–411. MR MR2423861
- [40] Antoine Joux, Sébastien Kunz-Jacques, Frédéric Muller, and Pierre-Michel Ricordel, *Cryptanalysis of the tractable rational map cryptosystem*, Public Key Cryptography—PKC 2005, Lecture Notes in Comput. Sci., vol. 3386, Springer, Berlin, 2005, pp. 258–274. MR MR2174046
- [41] Arkadius Kalka, Mina Teicher, and Boaz Tsaban, *Cryptanalysis of the algebraic eraser and short expressions of permutations as products*, 2008.
- [42] Wolfgang Lempken and Tran van Trung, *On minimal logarithmic signatures of finite groups*, Experiment. Math. **14** (2005), no. 3, 257–269. MR MR2172704

- [43] Françoise Levy-dit-Vehel and Ludovic Perret, *Polynomial equivalence problems and applications to multivariate cryptosystems*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 235–251. MR MR2092385 (2005e:94175)
- [44] Françoise Levy-dit Vehel and Ludovic Perret, *A Polly Cracker system based on satisfiability*, Coding, cryptography and combinatorics, Progr. Comput. Sci. Appl. Logic, vol. 23, Birkhäuser, Basel, 2004, pp. 177–192. MR MR2090648 (2005e:94176)
- [45] Le Van Ly, *Polly Two: A new algebraic polynomial-based public-key scheme*, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 3-4, 267–283. MR MR2233786
- [46] Mohamed Saied Emam Mohamed, Jintai Ding, and Johannes Buchmann, *Algebraic cryptanalysis of MQQ public key cryptosystem by mutantxl*, 2008.
- [47] Naoki Ogura and Shigenori Uchiyama, *Remarks on the attack of Fouque et al. against the LIC scheme*, 2008.
- [48] ———, *Cryptanalysis of the birational permutation signature scheme over a non-commutative ring*, 2009.
- [49] Ayoub Otmani, Jean-Pierre Tillich, and Leonard Dallot, *Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes*, 2008.
- [50] Ayoub Otmani, Jean-Pierre Tillich, and Léonard Dallot, *Cryptanalysis of two McEliece cryptosystems based on quasi-cyclic codes*, Math. Comput. Sci. **3** (2010), no. 2, 129–140.
- [51] Ludovic Perret, *A fast cryptanalysis of the isomorphism of polynomials with one secret problem*, Advances in Cryptology - Eurocrypt 2005, Lecture Notes in Computer Science, vol. 3494, Springer Berlin/Heidelberg, 2005, pp. 354–370.
- [52] Albrecht Petzoldt and Johannes Buchmann, *A multivariate signature scheme with an almost cyclic public key*, 2007.
- [53] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann, *Selecting parameters for the rainbow signature scheme – Extended version*, 2010, p. 21.
- [54] Benjamin Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, Advances in Cryptology, Eurocrypt 2008, Lecture Notes in Computer Science, vol. 4965, Springer Berlin/Heidelberg, 2008, pp. 163–180.



- [55] Rainer Steinwandt, *Loopholes in two public key cryptosystems using the modular group*, Public Key Cryptography (Cheju Island, 2001), Lecture Notes in Comput. Sci., vol. 1992, Springer, Berlin, 2001, pp. 180–189. MR MR1898034
- [56] ———, *A ciphertext-only attack on Polly Two*, Appl. Algebra Engrg. Comm. Comput. **21** (2010), no. 2, 85–92. MR 2600705 (2011b:94046)
- [57] Rainer Steinwandt and Regine Endsuleit, *A note on timing attacks based on the evaluation of polynomials*, 2000.
- [58] Rainer Steinwandt, Willi Geiselmann, and Regine Endsuleit, *Attacking a polynomial-based cryptosystem: Polly cracker*, Int. J. Inf. Secur. **1** (2002), no. 3, 143–148.
- [59] Shigeo Tsujii, Kohtaro Tadaki, and Ryou Fujita, *Proposal for piece in hand matrix: General concept for enhancing security of multivariate public key cryptosystems*, IE-ICE Trans A: Fundamentals **E90-A** (2007), no. 5, 992–999.
- [60] Shigeo Tsujii, Kohtaro Tadaki, and Ryou Fujita, *Nonlinear piece-in-hand matrix method for enhancing security of multivariate public key cryptosystems*, 2008.
- [61] Shigeo Tsujii, Kohtaro Tadaki, Masahito Gotaishi, Ryo Fujita, and Masao Kasahara, *Proposal of PPS multivariate public key cryptosystems*, 2009, p. 21 pages.
- [62] Valérie Gauthier Umaña and Gregor Leander, *Practical key recovery attacks on two McEliece variants*, 2009, pp. 1–19.
- [63] Eric R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), no. 4, 277–296. MR MR2090558
- [64] Zhiwei Wang, Xuyun Nie, Shihui Zheng, Yixian Yang, and Zhihui Zhang, *A new construction of multivariate Public Key Encryption Scheme through internally perturbed plus*, Computational Science and Its Applications, ICCSA 2008, Lecture Notes in Computer Science, vol. 5073, Springer, 2008, pp. 1–13.
- [65] Christopher Wolf, An Braeken, and Bart Preneel, *Efficient cryptanalysis of RSE(2) PKC and RSSE(2) PKC*, Security in Communication Networks: Fourth International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Lecture Notes in Comput. Sci., vol. 3352, Springer, Berlin, 2005, pp. 294–309.
- [66] ———, *On the security of stepwise triangular systems*, Des. Codes Cryptogr. **40** (2006), no. 3, 285–302. MR MR2251321

- [67] W. Christopher Wolf, *Multivariate quadratic polynomials in public key cryptography*, 2005.
- [68] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.
- [69] Kenneth Koon-Ho Wong, Gregory V. Bard, and Robert H. Lewis, *Partitioning multivariate polynomial equations via vertex separators for algebraic cryptanalysis and mathematical applications*, 2009.
- [70] Bo-Yin Yang, Chen-Mou Cheng, Bor-Rong Chen, and Chen Jiun-Ming, *Implementing minimized multivariate public-key cryptosystems on low-resource embedded systems*, 2005.

## Curve-Based Cryptography

- [1] Toru Akishita, Masanobu Katagi, Izuru Kitamura, and Tsuyoshi Takagi, *Some improved algorithms for hyperelliptic curve cryptosystems using degenerate divisors*, Information Security and Cryptology. ICISC 2004: 7th International Conference, Seoul, Korea, December 2–3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, p. 296.
- [2] Christine Abegail Antonio, Satoru Nakamura, and Ken Nakamura, *Comparing implementation efficiency of ordinary and squared pairings*, IACR eprint:2007:457 (2007).
- [3] Christine Abegail Antonio, Satoru Tanaka, and Ken Nakamura, *Implementing cryptographic pairings over curves of embedding degrees 8 and 10*, 2007.
- [4] Seigo Arita, Kazuto Matsuo, Koh-ichi Nagao, and Mahoro Shimura, *A Weil descent attack against elliptic curve cryptosystems over quartic extension fields*, IEICE Trans. Fundamentals **E89-A** (2006), no. 5, 28.
- [5] Daniel V. Bailey, Brian Baldwin, Lejla Batina, Daniel J. Bernstein, Peter Birkner, Joppe W. Bos, Gauthier van Damme, Giacomo de Meulenaer, Junfeng Fan, Tim Gneysu, Frank Gurkaynak, Thorsten Kleinjung, Tanja Lange, Nele Mentens, Christof Paar, Francesco Regazzoni, Peter Schwabe, and Leif Uhsadel, *The Certicom Challenges ECC2-X*, Tech. report, 2009.
- [6] M. Barbosa, A. Moss, and D. Page, *Compiler assisted elliptic curve cryptography*, On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, Lecture Notes in Computer Science, vol. 4804/2007, Springer Berlin / Heidelberg, 2007, pp. 1785–1802.
- [7] ———, *Constructive and destructive use of compilers in elliptic curve cryptography*, J. Cryptology **Online first** (2008), 23.
- [8] Paulo S. L. M. Barreto, B. Lynn, and M. Scott, *Constructing elliptic curves with prescribed embedding degrees*, Security in Communication Networks: Third International Conference, SCN 2002, Amalfi, Italy, September 11-13, 2002. Revised Papers., Lecture Notes in Comput. Sci., vol. 2576, Springer, Berlin, 2003, p. 257.

- [9] Abdolali Basiri, Andreas Enge, Jean-Charles Faugère, and Nicolas Gürel, *Implementing the arithmetic of  $C_{3,4}$  curves*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 87–101. MR MR2137346 (2006a:14101)
- [10] Mark Bauer, Edlyn Teske, and Annegret Weng, *Point counting on Picard curves in large characteristic*, Math. Comp. **74** (2005), no. 252, 1983–2005 (electronic). MR MR2164107
- [11] Daniel J. Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, Progress in cryptology—INDOCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4859, Springer, Berlin, 2007, pp. 167–182. MR MR2570254
- [12] Daniel J. Bernstein and Tanja Lange, *Faster addition and doubling on elliptic curves*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 29–50.
- [13] Peter Birkner, *Efficient arithmetic on low-genus curves*, Ph D thesis, Technische Universiteit Eindhoven, 2009.
- [14] Friederike Brezing and Annegret Weng, *Elliptic curves suitable for pairing based cryptography*, Des. Codes Cryptogr. **37** (2005), no. 1, 133–141. MR MR2165045
- [15] Ezra Brown, Bruce T. Myers, and Jerome A. Solinas, *Hyperelliptic curves with compact parameters*, Des. Codes Cryptogr. **36** (2005), no. 3, 245–261. MR MR2162578
- [16] Kyo Il Chung, Mun-Kyu Lee, Kunsoo Park, and Tae Jun Park, *Speeding up scalar multiplication in genus 2 hyperelliptic curves with efficient endomorphisms*, ETRI **27** (2005), no. 5, 617–627.
- [17] S. Cui, P. Duan, and C. W. Chan, *A new method of building more non-supersingular elliptic curves*, Computational Science and Its Applications, Lecture Notes in Comput. Sci., vol. 3481, Springer, Berlin, 2005, p. 657.
- [18] Jan Denef and Frederik Vercauteren, *An extension of Kedlaya’s algorithm to Artin-Schreier curves in characteristic 2*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 308–323. MR MR2041093 (2005d:11088)
- [19] Claus Diem, *The GHS attack in odd characteristic*, J. Ramanujan Math. Soc. **18** (2003), no. 1, 1–32. MR MR1966526 (2004a:14030)

- [20] ———, *An index calculus algorithm for plane curves of small degree*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 543–557. MR MR2282948
- [21] Claus Diem and Emmanuel Thomé, *Index calculus in class groups of non-hyperelliptic curves of genus three*, J. Cryptology **21** (2008), no. 4, 593–611. MR MR2438510
- [22] Régis Dupont, Andreas Enge, and François Morain, *Building curves with arbitrary small MOV degree over finite prime fields*, J. Cryptology **18** (2005), no. 2, 79–89. MR MR2148052 (2006c:11073)
- [23] I. Duursma, P. Gaudry, and F. Morain, *Speeding up the discrete log computation on curves with automorphisms*, Advances in Cryptology—Asiacrypt’99 (Singapore), Lecture Notes in Comput. Sci., vol. 1716, Springer, Berlin, 1999, pp. 103–121. MR MR1773225
- [24] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, Ser. Number Theory Appl., vol. 5, World Sci. Publ., Hackensack, NJ, 2008, pp. 1–28. MR MR2484046
- [25] David Freeman, *Constructing pairing-friendly genus 2 curves with ordinary Jacobians*, Pairing-based cryptography—Pairing 2007, Lecture Notes in Comput. Sci., vol. 4575, Springer, Berlin, 2007, pp. 152–176. MR MR2423638
- [26] David Freeman, Michael Scott, and Edlyn Teske, *A taxonomy of pairing-friendly elliptic curves*, Journal of Cryptology **23** (2010), no. 2, 224–280.
- [27] S. Galbraith, F. Hess, and F. Vercauteren, *Aspects of pairing inversion*, IEEE Transactions on Information Theory **54** (2008), no. 12, 5719–5728.
- [28] S. D. Galbraith, X. Lin, and D. J. Mireles, *Pairings on hyperelliptic curves with a real model*, LNCS 5209, Eds. Galbraith, S. D. and Paterson, K. G., Springer, 2008, pp. 256–281.
- [29] Steven Galbraith, *Disguising tori and elliptic curves*, 2006.
- [30] Steven D. Galbraith, *Supersingular curves in cryptography*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 495–513. MR MR1934860 (2004b:14037)

- [31] ———, *Weil descent of Jacobians*, Discrete Appl. Math. **128** (2003), no. 1, 165–180, International Workshop on Coding and Cryptography (WCC 2001) (Paris). MR MR1991424 (2004m:14046)
- [32] Steven D. Galbraith, Michael Harrison, and David J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 342–356. MR MR2467851 (2010f:14024)
- [33] Steven D. Galbraith, Florian Hess, and Nigel P. Smart, *Extending the GHS Weil descent attack*, Advances in Cryptology—Eurocrypt 2002 (Amsterdam), Lecture Notes in Comput. Sci., vol. 2332, Springer, Berlin, 2002, pp. 29–44. MR MR1975526 (2004f:94060)
- [34] Steven D. Galbraith, Xibin Lin, and David J. Mireles Morales, *Pairings on hyperelliptic curves with a real model*, Pairing-Based Cryptography, Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 265–281.
- [35] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, 2005.
- [36] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46. MR MR1880933 (2003b:14032)
- [37] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler, and A. Weng, *The 2-adic CM method for genus 2 curves with application to cryptography*, Advances in cryptology—ASIACRYPT 2006, Lecture Notes in Comput. Sci., vol. 4284, Springer, Berlin, 2006, pp. 114–129. MR MR2444631 (2009j:94110)
- [38] Pierrick Gaudry, *An algorithm for solving the discrete log problem on hyperelliptic curves*, Advances in Cryptology—Eurocrypt 2000 (Bruges), Lecture Notes in Comput. Sci., vol. 1807, Springer, Berlin, 2000, pp. 19–34. MR MR1772021
- [39] ———, *Index calculus for abelian varieties and the elliptic curve discrete logarithm problem*, 2004.
- [40] Pierrick Gaudry and Nicolas Gürel, *An extension of Kedlaya’s point-counting algorithm to superelliptic curves*, Advances in Cryptology—Asiacrypt 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494. MR MR1934859 (2003h:11159)

- [41] Pierrick Gaudry and Éric Schost, *Construction of secure random curves of genus 2 over prime fields*, Advances in Cryptology—EuroCrypt 2004, Lecture Notes in Comput. Sci., vol. 3027, Springer, Berlin, 2004, pp. 239–256. MR MR2153176
- [42] R. Granger and F. Vercauteren, *On the discrete logarithm problem on algebraic tori*, Crypto 2005: 25th Annual International Cryptology Conference (Santa Barbara, Cal., Lecture Notes in Comput. Sci., vol. 3621, Springer, Berlin, 2005, p. 66.
- [43] Robert Granger, *On the static Diffie-Hellman problem on elliptic curves over extension fields*, Advances in Cryptology - ASIACRYPT 2010 (Masayuki Abe, ed.), Lecture Notes in Computer Science, vol. 6477, Springer Berlin/Heidelberg, 2010, pp. 283–302.
- [44] Nicolas Gürel, *Extracting bits from coordinates of a point of an elliptic curve*, 2005.
- [45] Darrel Hankerson, Koray Karabina, and Alfred Menezes, *Analyzing the Galbraith-Lin-Scott point multiplication method for elliptic curves over binary fields*, 2008.
- [46] David Harvey, *Kedlaya’s algorithm in larger characteristic*, Int. Math. Res. Not. IMRN (2007), no. 22, Art. ID rnm095, 29. MR MR2376210
- [47] F. Hess, *Weil descent attacks*, Advances in Elliptic Curve Cryptography, London Math. Soc. Lecture Note Ser., vol. 317, Cambridge Univ. Press, Cambridge, 2005, pp. 151–180. MR MR2169214
- [48] Laura Hitt, *Families of genus 2 curves with small embedding degree*, J. Math. Cryptol. **3** (2009), no. 1, 19–36. MR MR2524253
- [49] Koh ichi Nagao, *Decomposed attack for the jacobian of a hyperelliptic curve over an extension field*, 2007.
- [50] Farzali A. Izadi and V. Kumar Murty, *Counting points on an abelian variety over a finite field*, Progress in Cryptology—Indocrypt 2003, Lecture Notes in Comput. Sci., vol. 2904, Springer, Berlin, 2003, pp. 323–333. MR MR2092391 (2005f:11127)
- [51] Waldyr D. Benits Junior and Steven D. Galbraith, *Constructing pairing-friendly elliptic curves using Gröbner basis reduction*, Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887/2007, Springer Berlin / Heidelberg, 2007, pp. 336–345.
- [52] Koray Karabina and Edlyn Teske, *On prime-order elliptic curves with embedding degrees  $k=3,4$ , and 6*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 102–117.

- [53] Masanobu Katagi, Toru Akishita, Izuru Kitamura, and Tsuyoshi Takagi, *Efficient hyperelliptic curve cryptosystems using theta divisors*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 151–160.
- [54] Masanobu Katagi, Izuru Kitamura, and Tsuyoshi Takagi, *A point halving algorithm for hyperelliptic curves*.
- [55] David R. Kohel, *The AGM- $X_0(N)$  Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)
- [56] Tanja Lange and Marc Stevens, *Efficient doubling on genus two curves over binary fields*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 3357, Springer, Berlin, 2005, pp. 170–181. MR MR2181316
- [57] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park, *Efficient and generalized pairing computation on abelian varieties*, IEEE Trans. Inform. Theory **55** (2009), no. 4, 1793–1803. MR MR2582765
- [58] Reynald Lercier and David Lubicz, *A quasi-quadratic time algorithm for hyperelliptic curve point counting*, Ramanujan J. **12** (2006), no. 3, 399–423. MR MR2293798 (2008b:11069)
- [59] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)
- [60] Markus Maurer, Alfred Menezes, and Edlyn Teske, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree (extended abstract)*, Progress in Cryptology—Indocrypt 2001 (Chennai), Lecture Notes in Comput. Sci., vol. 2247, Springer, Berlin, 2001, pp. 195–213. MR MR1934497
- [61] ———, *Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree*, LMS J. Comput. Math. **5** (2002), 127–174 (electronic). MR MR1942257 (2003k:94034)
- [62] J. Miret, D. Sadornil, J. Tena, R. Tomàs, and M. Valls, *Isogeny cordillera algorithm to obtain cryptographically good elliptic curves*, ACSW '07: Proceedings of the fifth



- Australasian symposium on ACSW frontiers, Australian Computer Society, Inc., 2007, pp. 153–157.
- [63] Nadia El Mrabet, Nicolas Guillermín, and Sorina Ionica, *A study of pairing computation for curves with embedding degree 15*, 2009.
- [64] A. Muzereau, N. P. Smart, and F. Vercauteren, *The equivalence between the DHP and DLP for elliptic curves used in practical applications*, LMS J. Comput. Math. **7** (2004), 50–72 (electronic). MR MR2047214 (2005b:94038)
- [65] Laura Hitt O’Connor, Gary McGuire, Michael Naehrig, and Marco Streng, *CM construction of genus 2 curves with  $p$ -rank 1*, 2008.
- [66] Tae-Jun Park, Mun-Kyu Lee, and Kunsoo Park, *Efficient scalar multiplication in hyperelliptic curves using a new Frobenius expansion*, ICISC 2003: Information Security and Cryptology, Lecture Notes in Comput. Sci., vol. 2971, Springer, Berlin, 2004, pp. 152–165. MR MR2093706 (2005f:94116)
- [67] L. J. D. Perez, Ezekiel J. Kachisa, and Michael Scott, *Implementing cryptographic pairings: A Magma tutorial*, 2009.
- [68] Tanaka Satoru and Nakamura Ken, *More constructing pairing-friendly elliptic curves for cryptography*, 2007.
- [69] Jasper Scholten, *Weil restriction of an elliptic curve over a quadratic extension*, 2004.
- [70] Michael Scott and Paulo S. L. M. Barreto, *On a (flawed) proposal to build more pairing-friendly curves*, 2005.
- [71] Katsuyuki Takashima, *New families of hyperelliptic curves with efficient Gallant-Lambert-Vanstone method*, Information Security and Cryptology, ICISC 2004: 7th International Conference, Seoul, Korea, December 2-3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, pp. 279–295.
- [72] Katsuyuki Takashima, *A new type of fast endomorphisms on Jacobians of hyperelliptic curves and their cryptographic application*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 124–133.
- [73] ———, *Scaling security of elliptic curves with fast pairing using efficient endomorphisms*, IEICE Trans. Fundamentals **E-90A** (2007), no. 1, 152–159.

- [74] ———, *Efficiently computable distortion maps for supersingular curves*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer Berlin/Heidelberg, 2008, pp. 88–101.
- [75] Satoru Tanaka and Ken Nakamura, *Constructing pairing-friendly elliptic curves using factorization of cyclotomic polynomials*, Pairing-Based Cryptography, Pairing 2008, Lecture Notes in Computer Science, vol. 5209, Springer, 2008, pp. 136–145.
- [76] Edlyn Teske, *An elliptic curve trapdoor system (extended abstract)*, High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, Fields Inst. Commun., vol. 41, Amer. Math. Soc., Providence, RI, 2004, pp. 341–352. MR MR2076258
- [77] ———, *An elliptic curve trapdoor system*, J. Cryptology **19** (2006), no. 1, 115–133. MR MR2210901 (2006k:94116)
- [78] Frederik Vercauteren, *The hidden root problem*, Pairing-Based Cryptography - Pairing, Lecture Notes in Computer Science, vol. 5209, SpringerLink, Berlin, 2008, pp. 89–99. MR )
- [79] Eric R. Verheul, *Evidence that XTR is more secure than supersingular elliptic curve cryptosystems*, J. Cryptology **17** (2004), no. 4, 277–296. MR MR2090558
- [80] Annegret Weng, *Generation of random Picard curves for cryptography*, 2004.
- [81] ———, *A low-memory algorithm for point counting on Picard curves*, Des. Codes Cryptogr. **38** (2006), no. 3, 383–393. MR MR2195523 (2006j:11168)
- [82] Fangguo Zhang, *Twisted ate pairing on hyperelliptic curves and applications*, 2008.
- [83] Chang-An Zhao, Fangguo Zhang, and Jiwu Huang, *All pairings are in a group*, IEICE Trans A: Fundamentals **E91-A** (2008), no. 10, 3084–3087.

## Protocols

- [1] Gregory V. Bard, *The application of polynomials over the field of two elements to a problem in intellectual property*, 2009.
- [2] S.T. Dougherty, S. Mesnager, and P. Sole, *Secret-sharing schemes based on self-dual codes*, Information Theory Workshop, 2008. ITW '08. IEEE (2008), 338–342.
- [3] Greg Gamble, Barbara M. Macnhaut, Jennifer Seberry, and Anne Penfold Street, *Further results on strongbox secured secret sharing schemes*, Util. Math. **66** (2004), 165–193. MR MR2106217 (2005g:94090)
- [4] Shuhui Hou, Tetsutaro Uehara, Yoshitaka Morimura, and Michihiko Minoh, *Fingerprinting codes for live pay-television broadcast via internet*, Multimedia Content Analysis and Mining, Lecture Notes in Computer Science, vol. 4577/2007, Springer Berlin / Heidelberg, 2007, pp. 252–261.
- [5] David Jao and Kayo Yoshida, *Boneh-Boyen signatures and the strong Diffie-Hellman problem*, 2009.
- [6] Antoine Joux, Reynald Lercier, David Naccache, and Emmanuel Thomé, *Oracle-assisted static Diffie-Hellman is easier than discrete logarithms*, 2008.
- [7] Kerem Kaskaloglu and Ferruh Özbudak, *A simple scheme for hierarchical threshold access structures*, 2009, p. 8.
- [8] Matthias Krause and Dirk Stegemann, *More on the security of linear RFID authentication protocols*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 5867, Springer, Berlin, 2009, pp. 182–196.
- [9] Sihem Mesnager, P. Solé, and Steven T. Dougherty, *Secret sharing schemes based on self-dual codes*, Information Theory Workshop, 2008. ITW '08. IEEE (2008), 338 – 342.
- [10] Rainer Steinwandt and Viktória I. Villányi, *A one-time signature using run-length encoding*, Inform. Process. Lett. **108** (2008), no. 4, 179–185. MR MR2457922
- [11] Suratose Tritilanunt, Colin Boyd, Ernest Foo, and Juan Manuel González Nieto, *Toward non-parallelizable client puzzles*, Cryptology and Network Security, Lecture Notes in Computer Science, vol. 4856/2007, Springer, Berlin/Heidelberg, 2007, pp. 247–264.

## Random Number Generators

- [1] Michael Feng-Hao Liu, Chi-Jen Lu, Bo-Yin Yang, and Jintai Ding, *Secure PRNGs from specialized polynomial maps over any  $F_q$* , 2007.
- [2] D. Schellekens, B. Preneel, and I. Verbauwhede, *FPGA vendor agnostic true random number generator*, Field Programmable Logic and Applications, 2006. FPL '06 (2006).

## Computational Methods

- [1] Gwénolé Ars, Jean-Charles Faugère, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita, *Comparison between XL and Gröbner basis algorithms*, Advances in Cryptology—Asiacrypt 2004, Lecture Notes in Comput. Sci., vol. 3329, Springer, Berlin, 2004, pp. 338–353. MR MR2150425 (2006k:13056)
- [2] Roberto Maria Avanzi, *Another look at square roots (and other less common operations) in fields of even characteristic*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 138–154.
- [3] M. Barbosa, R. Noad, D. Page, and N. P. Smart, *First steps toward a cryptography-aware language and compiler*.
- [4] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson, *Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over  $\text{GF}(2)$  via SAT-solvers*, 2007.
- [5] Aurélie Bauer and Antoine Joux, *Toward a rigorous variation of Coppersmith’s algorithm on three variables*, Advances in cryptology—EUROCRYPT 2007, Lecture Notes in Comput. Sci., vol. 4515, Springer, Berlin, 2007, pp. 361–378. MR MR2449220
- [6] Stanislav Bulygin and Michael Brickenstein, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, 2008.
- [7] Wouter Castryck, Hendrik Hubrechts, and Frederik Vercauteren, *Computing zeta functions in families of  $C_{a,b}$  curves using deformation*, Algorithmic Number Theory, Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 296–311.
- [8] Chia-Hsin Owen Chen, Ming-Shing Chen, Jintai Ding, Fabian Werner, and Bo-Yin Yang, *Odd-char multivariate hidden field equations*, 2008.
- [9] Jiun-Ming Chen and Bo-Yin Yang, *All in the XL family: Theory and practice*, Information Security and Cryptology. ICISC 2004: 7th International Conference, Seoul, Korea, December 2–3, 2004, Lecture Notes in Comput. Sci., vol. 3506, Springer, Berlin, 2005, p. 296.
- [10] Jean-Charles Faugère and Ludovic Perret, *Algebraic cryptanalysis of Curry and Flurry using correlated messages*, 2008.

- [11] Antoine Joux, David Naccache, and Emmanuel Thomé, *When  $e$ -th roots become easier than factoring*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833/2007, Springer Berlin / Heidelberg, 2007, pp. 13–28.
- [12] David R. Kohel, *The AGM- $X_0(N)$  Heegner point lifting algorithm and elliptic curve point counting*, Advances in Cryptology—Asiacrypt 2003, Lecture Notes in Comput. Sci., vol. 2894, Springer, Berlin, 2003, pp. 124–136. MR MR2093256 (2005i:11077)
- [13] Czesław Kościelny, *Computing in the composite  $\text{GF}(q^m)$  of characteristic 2 formed by means of an irreducible binomial*, Appl. Math. Comput. Sci. **8** (1998), no. 3, 671–680. MR MR1647512 (99i:94047)
- [14] Kazuto Matsuo, Jinhui Chao, and Shigeo Tsujii, *An improved baby step giant step algorithm for point counting of hyperelliptic curves over finite fields*, Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 461–474. MR MR2041104 (2005a:11089)
- [15] Mohamed Saied Emam Mohamed, Wael Said Abd Elmageed Mohamed, Jintai Ding, and Johannes Buchmann, *MXL2: Solving polynomial equations over  $\text{GF}(2)$  using an improved mutant strategy*, Post-Quantum Cryptography, Lecture Notes in Comput. Sci., vol. 5299, Springer, Berlin, 2008, pp. 203–215.
- [16] Naoki Ogura and Shigenori Uchiyama, *Cryptanalysis of the birational permutation signature scheme over a non-commutative ring*, 2009.
- [17] Mikael Olofsson, *Vlsi Aspects on Inversion in Finite Fields*, PhD Thesis, Linköpings Universitet, Linköping, Sweden, 2002.
- [18] Håvard Raddum and Igor Semaev, *Solving multiple right hand sides linear equations*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 147–160. MR MR2438447
- [19] A. J. M. Segers, *Algebraic Attacks from a Gröbner Basis Perspective*, MSc Thesis, Technische Universiteit Eindhoven, 2004.
- [20] Igor Semaev, *Sparse boolean equations and circuit lattices*, 2009.
- [21] B. Smith, *Isogenies and the discrete logarithm problem in Jacobians of genus 3 hyperelliptic curves*, J. Cryptology **22** (2009), no. 4, 505–529.

- [22] Makoto Sugita, Mitsuru Kawazoe, and Hideki Imai, *Relation between the XL algorithm and Groebner basis algorithms*, IEICE Trans. Fundamentals **E89-A** (2006), no. 1, 11–18.
- [23] Kenneth Koon-Ho Wong, Gregory V. Bard, and Robert H. Lewis, *Partitioning multivariate polynomial equations via vertex separators for algebraic cryptanalysis and mathematical applications*, 2009.

# Information and Communication

## Information

94Axx except 94A60, 94A62

- [1] Alin Bostan, Pierrick Gaudry, and Éric Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, Finite Fields and Applications, Lecture Notes in Comput. Sci., vol. 2948, Springer, Berlin, 2004, pp. 40–58. MR MR2092621
- [2] Michael Clausen, *Fast Fourier transforms for metabelian groups*, SIAM J. Comput. **18** (1989), no. 3, 584–593. MR MR996838 (90e:94002)
- [3] Jean-Charles Faugère, François Moreau de Saint-Martin, and Fabrice Rouillier, *Design of regular nonseparable bidimensional wavelets using Gröbner basis techniques*, IEEE Trans. Signal Process. **46** (1998), no. 4, 845–856. MR MR1665643
- [4] Gohar M. Kyureghyan and Alexander Pott, *On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences*, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 149–164. MR MR1993164 (2004g:94036)
- [5] San Ling and Patrick Solé, *Nonlinear  $p$ -ary sequences*, Appl. Algebra Engrg. Comm. Comput. **14** (2003), no. 2, 117–125. MR MR1995563 (2004g:94040)
- [6] Eva Nuria Müller, *On the crosscorrelation of sequences over  $\text{GF}(p)$  with short periods*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 289–295. MR MR1677872 (2000f:94021)
- [7] Jonas Samuelsson, *Multidimensional companding quantization of the Gaussian source*, IEEE Trans. Inform. Theory **49** (2003), no. 5, 1343–1351. MR MR1984833 (2004e:94025)
- [8] Chaoping Xing, *Applications of algebraic curves to constructions of sequences*, Cryptography and Computational Number Theory (Singapore, 1999), Progr. Comput. Sci. Appl. Logic, vol. 20, Birkhäuser, Basel, 2001, pp. 137–146. MR MR1944725 (2004e:11068)



# Circuits and Networks

94Cxx

- [1] François Arnault and Thierry P. Berger, *Design and properties of a new pseudorandom generator based on a filtered FCSR automaton*, IEEE Trans. Comput **54** (2005), no. 11, 1374–1383.
- [2] Willi Geiselmann, Jörn Müller-Quade, and Rainer Steinwandt, *Comment on: “A new representation of elements of finite fields  $\text{GF}(2^m)$  yielding small complexity arithmetic circuits” by G. Drolet*, IEEE Trans. Comput. **51** (2002), no. 12, 1460–1461. MR MR2012149
- [3] Willi Geiselmann and Rainer Steinwandt, *A redundant representation of  $\text{GF}(q^n)$  for designing arithmetic circuits*, IEEE Trans. Comp **52** (2003), no. 7, 848–853.
- [4] Stephen T. Schibell and Richard M. Stafford, *Processor interconnection networks from Cayley graphs*, Discrete Appl. Math. **40** (1992), no. 3, 333–357. MR MR1197007 (94a:68005)
- [5] Lewis Stiller, *Group graphs and computational symmetry on massively parallel architecture*, The Journal of Supercomputing (1991), no. 5, 99–117.
- [6] ———, *Exploiting Symmetry on Parallel Architectures*, Ph.D. thesis, John Hopkins University, 1995.

# Signal Processing

- [1] Michael Clausen, *Beiträge zum Entwurf schneller Spektraltransformationen*, Habilitationsschrift, Universität Karlsruhe, 1998.
- [2] Torsten Minkwitz, *Algorithmensynthese für lineare Systeme mit Symmetrie*, Dissertation, Technische Hochschule, Universität Karlsruhe, 1993.
- [3] Luciano Sbaiz, Patrick Vandewalle, and Martin Vetterli, *Groebner basis methods for multichannel sampling with unknown offsets*, Appl. Comput. Harmon. Anal. **25** (2008), no. 3, 277 – 294.
- [4] Benno Tietz, *Automatisierter Entwurf schneller Spektraltransformationen*, Diplomarbeit, Universität Karlsruhe, 1989.

# Data Mining

- [1] Daniel M. Gordon, Victor Miller, and Peter Ostapenko, *Optimal hash functions for approximate closest pairs on the  $n$ -cube*, 2008.

# Biology

## Mathematical Biology

92Bxx

- [1] Weronika Buczyńska, *Phylogenetic varieties on graphs*, 2010.
- [2] Nicholas Eriksson, *Toric ideals of homogeneous phylogenetic models*, ISSAC 2004, ACM, New York, 2004, pp. 149–154. MR MR2126937 (2005j:92017)
- [3] Nicholas Eriksson, *Algebraic Combinatorics for Computational Biology*, Ph.D. thesis, University of California, Berkeley, 2006, p. 135.
- [4] Reinhard Laubenbacher and Bernd Sturmfels, *Computer algebra in systems biology*, *American Mathematical Monthly* **116** (2009), no. 10, 882–891.

# Chemistry

## Chemistry

92Exx

- [1] Jean Brocas, Francis Buekenhout, and Michel Dehon, *Enantiomeric labelling of reaction graphs*, J. Chem. Inf. Comput. Sci. (1998), no. 38, 798–810.
- [2] A. Brown, A. B. McCoy, B. J. Braams, Z. Jin, and J. M. Bowman, *Quantum and classical studies of vibrational motion of  $\text{CH}_5^+$  on a global potential energy surface obtained from a novel ab initio direct dynamics approach*, J. Chem. Phys. **121** (2004), 4105–4116.
- [3] Chao Chen, Benjamin C. Shepler, Bastiaan J. Braams, and Joel M. Bowman, *Quasi-classical trajectory calculations of the  $\text{OH} + \text{NO}_2$  association reaction on a global potential energy surface*, J. Chem. Phys **127** (2007), no. 104310, 11 pages.
- [4] S. Fritzsche, *Application of point-group symmetries in chemistry and physics: A computer-algebraic approach*, Int. J. Quantum. Chem **106** (2006), 98–129.
- [5] Modjtaba Ghorbani and Ali Reza Ashrafi, *Counting the number of hetero fullerenes*, Journal of Computational and Theoretical Nanoscience **3** (2006), no. 5, 803–810.
- [6] Xinchuan Huang, Bastiaan J. Braams, and Joel M. Bowman, *Ab initio potential energy and dipole moment surfaces for  $\text{H}_5\text{O}_2^+$* , J. Chem. Phys **122** (2005), no. 044308, 12 pages.
- [7] K. Kutnar, A. Malnič, and Dragan Marušič, *Chirality of toroidal molecular graphs*, J. Chem. Inf. Model. **45** (2005), no. 6, 1527–1535. MR MR1687732
- [8] Amit R. Sharma, Bastiaan J. Braams, Stuart Carter, Benjamin C. Shepler, and Joel M. Bowman, *Full-dimensional ab initio potential energy surface and vibrational configuration interaction calculations for vinyl*, J. Chem. Phys **130** (2009), no. 174301, 9 pages.
- [9] Amit R. Sharma, J. Wu, B. J. Braams, S. Carter, R. Schneider, B. Shepler, and J. M. Bowman, *Potential energy surfaces and MULTIMODE vibrational analysis of  $\text{C}_2\text{H}_3^+$* , J Chem Phys. **125** (2006), 224306.

- [10] Yimin Wang, Bastiaan J. Braams, Joel M. Bowman, Stuart Carter, and D. P. Tew, *Full-dimensional quantum calculations of ground-state tunneling splitting of malonaldehyde using an accurate ab initio potential energy surface*, J. Chem. Phys **128** (2008), no. 224314, 9 pages.
- [11] Yimin Wang, Stuart Carter, Bastiaan J. Braams, and Joel M. Bowman, *Multimode quantum calculations of intramolecular vibrational energies of the water dimer and trimer using ab initio-based potential energy surfaces*, J. Chem. Phys **128** (2008), no. 071101, 5 pages.
- [12] Yimin Wang, Benjamin C. Shepler, Bastiaan J. Braams, and Joel M. Bowman, *Full-dimensional, ab initio potential energy and dipole moment surfaces for water*, J. Chem. Phys **131** (2009), no. 054511, 8 pages.
- [13] Peng Zhang, Satoshi Maeda, Keiji Morokuma, and Bastiaan J. Braams, *Photochemical reactions of the low-lying excited states of formaldehyde: T1/S0 intersystem crossings, characteristics of the S1 and T1 potential energy surfaces, and a global T1 potential energy surface*, J. Chem. Phys **130** (2009), no. 114304, 10 pages.

# Economics

## Mathematical Economics

91Bxx

- [1] Marston Conder and Arkadii Slinko, *A counterexample to Fishburn's conjecture on finite linear qualitative probability*, J. Math. Psych. **48** (2004), no. 6, 425–431. MR MR2108382 (2006c:60006)
- [2] Jean-Paul Doignon and Michel Regenwetter, *On the combinatorial structure of the approval-voting polytope*, J. Math. Psych. **46** (2002), no. 5, 554–563. MR MR1931565 (2003k:91052)
- [3] Murat Sertel and Arkadii Slinko, *Ranking committees, income streams or multisets*, Economic Theory **30** (2007), no. 2, 265–287.

# Operations Research

## Operations Research

90Bxx

- [1] Levent Kandiller, *Principles of Mathematics in Operations Research*, International Series in Operations Research & Management Science, 97, Springer, New York, 2007. MR2263913



# Mathematical Programming

90Cxx

- [1] Karin Gatermann and Pablo A. Parrilo, *Symmetry groups, semidefinite programs, and sums of squares*, J. Pure Appl. Algebra **192** (2004), no. 1-3, 95–128. MR MR2067190 (2005d:68155)
- [2] Yan Wang, Xin Gui Fang, and D. F. Hsu, *On the edge-forwarding indices of Frobenius graphs*, Acta Math. Sin. (Engl. Ser.) **22** (2006), no. 6, 1735–1744. MR MR2262432

**Physics**  
**Mechanics**  
70Fxx

- [1] Marshall Hampton and Richard Moeckel, *Finiteness of stationary configurations of the four-vortex problem*, Trans. Amer. Math. Soc. **361** (2009), no. 3, 1317–1332.
- [2] Marshall Hampton and Manuele Santoprete, *Seven-body central configurations: A family of central configurations in the spatial seven-body problem*, Cel. Mec. Dynam. Astron **99** (2007), no. 4, 293–305.
- [3] I. Kotsireas and D. Lazard, *Central configurations of the 5-body problem with equal masses in three-dimensional space*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **258** (1999), no. Teor. Predst. Din. Sist. Komb. i Algoritm. Metody. 4, 292–317, 360–361. MR MR1755843 (2001b:70017)

# Quantum Theory

81Xxx except 81P68

- [1] Ingemar Bengtsson, Wojciech Bruzda, Asa Ericsson, Jan-Ake Larsson, Wojciech Tadej, and Karol Zyczkowski, *Mutually unbiased bases and Hadamard matrices of order six*, J. Math. Phys. **48** (2007), no. 052106, 1–21.
- [2] Markus Grassl, Martin Rötteler, and Thomas Beth, *Computing local invariants of quantum-bit systems*, Phys. Rev. A (3) **58** (1998), no. 3, 1833–1839. MR MR1643864 (99d:81026)
- [3] Dhagash B. Mehta, *Lattice vs. Continuum: Landau Gauge Fixing and 't Hooft-Polyakov Monopoles*, Phd thesis, University of Adelaide, 2010, pp. 1–149.
- [4] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves, *Symmetric informationally complete quantum measurements*, J. Math. Phys. **45** (2004), no. 6, 2171–2180. MR MR2059685 (2004m:81043)
- [5] H. E. Winkelkemper, *AP theory II: Intrinsic 4D quantum YM theory with mass gap*, 2007.
- [6] Pawel Wocjan, *Efficient decoupling schemes with bounded controls based on Eulerian orthogonal arrays*, Phy. Rev. A. **73** (2006), no. 6, 7.

# Quantum Computation

81P68

- [1] Thomas Beth, Christopher Charnes, Markus Grassl, Gernot Alber, Aldo Delgado, and Michael Mussinger, *A new class of designs which protect against quantum jumps*, Des. Codes Cryptogr. **29** (2003), no. 1-3, 51–70. MR MR1993156 (2004i:94065)
- [2] Marcus Palmer da Silva, *Erasure thresholds for efficient linear optics quantum computation*, Master's thesis, University of Waterloo, 2004.
- [3] G. David Forney, Jr., Markus Grassl, and Saikat Guha, *Convolutional and tail-biting quantum error-correcting codes*, IEEE Trans. Inform. Theory **53** (2007), no. 3, 865–880. MR MR2302801
- [4] M. Grassl, Thomas Beth, and T. Pellizzari, *Codes for the quantum erasure channel*, Phys. Rev. A (3) **56** (1997), no. 1, 33–38. MR MR1459695 (98f:81044)
- [5] M. Grassl, Thomas Beth, and M. Rötteler, *Computing local invariants of quantum-bit systems*, Phys. Rev. A. **58** (1998), no. 3, 833–1839.
- [6] Markus Grassl, *On SIC-POVMs and MUBs in dimension 6*, 2004.
- [7] Markus Grassl, *Tomography of quantum states in small dimensions*, Proceedings of the Workshop on Discrete Tomography and its Applications (Amsterdam), Electron. Notes Discrete Math., vol. 20, Elsevier, 2005, pp. 151–164 (electronic). MR MR2301093
- [8] Russell John Higgs, *Nice error bases and Sylow subgroups*, IEEE Trans. Inform. Theory **54** (2008), no. 9, 4199–4207. MR MR2450777
- [9] Min-Hsiu Hsieh, Igor Devetak, and Todd Brun, *General entanglement-assisted quantum error-correcting codes*, Physical Review A (Atomic, Molecular, and Optical Physics) **76** (2007), no. 6, 062313.
- [10] Andreas Klappenecker and Martin Rötteler, *Beyond stabilizer codes I: Nice error bases*, IEEE Trans. Inform. Theory **48** (2002), no. 8, 2392–2395. MR MR1930299 (2003k:94055)

- [11] ———, *Unitary error bases: Constructions, equivalence, and applications*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Toulouse, 2003), Lecture Notes in Comput. Sci., vol. 2643, Springer, Berlin, 2003, pp. 139–149. MR MR2042421 (2005c:94088)
- [12] ———, *On the structure of nonstabilizer Clifford codes*, Quantum Inf. Comput. **4** (2004), no. 2, 152–160. MR MR2065357 (2005h:94086)
- [13] Samuel J. Lomonaco, Jr. and Louis H. Kauffman, *Quantum hidden subgroup algorithms: A mathematical perspective*, Quantum Computation and Information (Washington, DC, 2000), Contemp. Math., vol. 305, Amer. Math. Soc., Providence, RI, 2002, pp. 139–202. MR MR1947336 (2004k:81097)
- [14] Jean-Gabriel Luque, Jean-Yves Thibon, and Frédéric Toumazet, *Unitary invariants of qubit systems*, Math. Structures Comput. Sci. **17** (2007), no. 6, 1133–1151. MR MR2372468
- [15] Gabriele Nebe, Eric M. Rains, and Neil J. A. Sloane, *Self-dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR MR2209183
- [16] Michel Planat, *Clifford group dipoles and the enactment of Weyl/Coxeter group  $W(E_8)$  by entangling gates*, 2009.
- [17] Michel Planat, Peter Levay, and Metod Saniga, *Balanced tripartite entanglement, the alternating group  $A_4$  and the Lie algebra  $sl(3, c) \oplus u(1)$* , 2009.
- [18] Thomas Schulte-Herbrüggen, Uwe Sander, and Robert Zeier, *Symmetry principles in quantum system theory of multi-qubit systems made simple*, Proceedings of the 4th International Symposium on Communications, Control and Signal Processing, ISCCSP 2010, Limassol, Cyprus, 3–5 March 2010, IEEE, 2010, pp. 1–5.
- [19] Thomas Schulte-Herbrüggen, Uwe Sander, , and Robert Zeier, *Symmetry principles in quantum system theory of multi-qubit systems made simple*, Communications, Control and Signal Processing, ISCCSP 2010. Proceedings of the 4th International Symposium, IEEE, 2010, pp. 1–5.
- [20] A. J. Scott and M. Grassl, *Symmetric informationally complete positive-operator-valued measures: A new computer study*, 2010, p. 042203.

- [21] Barbara M. Terhal, Isaac L. Chuang, David P. Di Vincenzo, Markus Grassl, and John A. Smolin, *Simulating quantum operations with mixed environments*, Phys. Rev **60** (1999), no. 2, 881–885. MR MR0000020
- [22] Pawel Wocjan, Martin Rötteler, Dominik Janzing, and Thomas Beth, *Universal simulation of Hamiltonians using a finite set of control operations*, Quantum Inf. Comput. **2** (2002), no. 2, 133–150. MR MR1910083 (2003e:81036)
- [23] Robert Michael Zeier, *Lie-theoretischer zugang zur erzeugung unitärer transformationen auf quantenrechnern*, Ph.D. thesis, Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 2006, p. 140.

# Statistical Mechanics

82Xxx

- [1] J. Buhler and Z. Reichstein, *Symmetric functions and the phase problem in crystallography*, Trans. Amer. Math. Soc. **357** (2005), no. 6, 2353–2377 (electronic). MR MR2140442
- [2] Bettina Eick and Bernd Souvignier, *Algorithms for crystallographic groups*, Int. J. Quantum. Chem **106** (2006), no. 1, 316–343.
- [3] Peter J. Forrester and Eric M. Rains, *Interrelationships between orthogonal, unitary and symplectic matrix ensembles*, Random matrix models and their applications, Math. Sci. Res. Inst. Publ., vol. 40, Cambridge Univ. Press, Cambridge, 2001, pp. 171–207. MR MR1842786 (2002h:82008)
- [4] S. Fritzsche, *Application of point-group symmetries in chemistry and physics: A computer-algebraic approach*, Int. J. Quantum. Chem **106** (2006), 98–129.
- [5] J. Opgenorth, W. Plesken, and T. Schulz, *Crystallographic algorithms and tables*, Acta Cryst. Sect. A **54** (1998), no. 5, 517–531. MR MR1645546 (99h:20082)
- [6] Craig A. Tracy, Larry Grove, and M. F. Newman, *Modular properties of the hard hexagon model*, J. Statist. Phys. **48** (1987), no. 3-4, 477–502. MR MR914893 (89b:82125)

# Relativity and Gravitation

- [1] J. S. Dowker and Peter Chang, *Analytic torsion on spherical factors and tessellations*.
- [2] Peter Lorimer, *Models for a finite universe*, *Internat. J. Theoret. Phys.* **41** (2002), no. 7, 1201–1274. MR MR1923298 (2003h:57020)
- [3] Francesco Dalla Piazza, *More on superstring chiral measures*, *Nuclear Physics B* **844** (2011), no. 3, 471–499.
- [4] A. A. Ungar, *Hyperbolic trigonometry in the Einstein relativistic velocity model of hyperbolic geometry*, *Comput. Math. Appl.* **40** (2000), no. 2-3, 313–332. MR MR1763628 (2001e:83005)
- [5] Abraham A. Ungar, *Beyond the Einstein Addition Law and its Gyroscopic Thomas Precession*, *Fundamental Theories of Physics*, vol. 117, Kluwer Academic Publishers Group, Dordrecht, 2001, The theory of gyrogroups and gyrovector spaces. MR MR1978122 (2004c:83006)
- [6] H.E. Winkelkemper, *AP Theory III: Cone-like graded SUSY, Dynamic Dark Energy and the YM Millenium problem*, 2010.



# Geophysics

86-xx

- [1] Joseph L. Awange and Erik W. Grafarend, *Solving Algebraic Computational Problems in Geodesy and Geoinformatics*, Springer-Verlag, Berlin, 2005, The answer to modern challenges. MR MR2139870 (2006b:86022)
- [2] D. W. Vasco, *Intersections, ideals, and inversion*, *Inverse Problems* **15** (1999), no. 6, 1573–1602. MR MR1733217 (2000i:86026)