A Selection of Books, Papers, and Theses
Citing Magma

Computational Algebra Group
University of Sydney

January 4, 2019
## Contents

**Overview of the Bibliography**

*Introduction* .................................................. 1

*Citing MAGMA in Publications* .................................. 1

*Bibliography Files* ........................................... 2

*Acknowledgements* ............................................ 2

**Mathematics**

**Algebraic Geometry** ........................................ 4

*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

**Algebraic Structures** ...................................... 36

*Ordered Structures* ........................................... 36

**Algebras – Associative** .................................... 37

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

Numerical Analysis ................................................. 292
All Areas .......................................................... 292

Probability and Statistics ...................................... 293
Probability ......................................................... 293
Statistics ........................................................ 295

Topological and Lie Groups ..................................... 296
Lie Groups ........................................................ 296
Noncompact Transformation Groups ....................... 297

Topology ........................................................... 298
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
## Coding Theory

- **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

## Computer Science

- **Computer System Organization** ................................................ 346
- **Software** .................................................................................. 347
- **Theory of Computing** ............................................................... 350
- **Artificial Intelligence** ............................................................... 352
- **Computing Methodologies** ......................................................... 355
- **Symbolic and Computational Algebra** ....................................... 356

## Cryptography

- **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

## Information and Communication

- **Information** ............................................................................. 385
- **Circuits and Networks** ............................................................ 386
- **Signal Processing** ................................................................. 387
- **Data Mining** ........................................................................... 388

## Physical and Social Sciences
<table>
<thead>
<tr>
<th>Field</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biology</td>
<td>389</td>
</tr>
<tr>
<td>Mathematical Biology</td>
<td>389</td>
</tr>
<tr>
<td>Chemistry</td>
<td>390</td>
</tr>
<tr>
<td>Chemistry</td>
<td>390</td>
</tr>
<tr>
<td>Economics</td>
<td>392</td>
</tr>
<tr>
<td>Mathematical Economics</td>
<td>392</td>
</tr>
<tr>
<td>Operations Research</td>
<td>393</td>
</tr>
<tr>
<td>Operations Research</td>
<td>393</td>
</tr>
<tr>
<td>Mathematical Programming</td>
<td>394</td>
</tr>
<tr>
<td>Physics</td>
<td>395</td>
</tr>
<tr>
<td>Mechanics</td>
<td>395</td>
</tr>
<tr>
<td>Quantum Theory</td>
<td>396</td>
</tr>
<tr>
<td>Quantum Computation</td>
<td>397</td>
</tr>
<tr>
<td>Statistical Mechanics</td>
<td>400</td>
</tr>
<tr>
<td>Relativity and Gravitation</td>
<td>401</td>
</tr>
<tr>
<td>Geophysics</td>
<td>402</td>
</tr>
</tbody>
</table>
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:


Alternatively, you could cite the MAGMA Handbook:


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:


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


Local Theory
14Bxx

Cycles and Subschemes
14Cxx


Families and Fibrations
14Dxx


14Exx


Arithmetic and Diophantine Geometry
14Gxx


[16] Xander Faber and Benjamin Hutz, On the number of rational iterated pre-images of the origin under quadratic dynamical systems, 2008.


Curves
14Hxx


[34] Aristides Kontogeorgis and Victor Rotger, On abelian automorphism groups of Mumford curves and applications to Shimura curves, 2006.


Surfaces and Higher Dimensional Varieties

14Jxx


[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.


Abelian Varieties and Schemes
14Kxx


Algebraic Groups
14Lxx


Special Varieties
14Mxx


Real Algebraic Geometry


Computational Methods
14-04, 14Qxx


Algebraic Structures
Ordered Structures

06Xxx


Algebras – Associative

Associative Algebras: General

16Bxx, 16Lxx, 16Nxx, 16Pxx


Orders and Arithmetic
16Hxx


Division Rings and Semisimple Artin Rings
16Kxx

Algebras from Standard Constructions

16Sxx


Computational Methods

16-04


Algebras – Non-Associative
Nonassociative Algebras: General
17Axx


Lie Algebras
17Bxx except 17B37


48
Quantum Groups

17B37


Computational Methods
17-04


Analysis
Analysis: General
26Xxx


Riemann Surfaces
30Fxx


Functions of Several Complex Variables
32Xxx


Ordinary Differential Equations
34Xxx


Partial Differential Equations
35Xxx


Combinatorics
Enumerative Combinatorics
05Axx


Designs and Configurations

05Bxx


[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)


[58] J. D. Key and K. Mackenzie, Ovals in the designs $W(2^m)$, Ars Combin. 33 (1992), 113–117. MR MR1174835 (93d:05035)


70


[75] Wolfgang Lempken, *Two new symmetric 2-(144, 66, 30) designs*.


Graph Theory

05Cxx


[54] Alice Devillers, Michael Giudici, Cai Heng Li, and Cheryl E. Praeger, *A remarkable Mathieu graph tower*.


References


Invariant Theory
13A50


Homological Methods
13Dxx


Differential Algebra
12H05, 13Nxx


[64] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions.*


Field Theory

Field Theory: General

12Exx


Extensions and Galois Theory

12Fxx


Semifields and Near-fields
12Kxx


Geometry
Incidence Geometry
51Axx, 51Bxx


Finite Geometry
51Exx


[64] 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)


126


A generalization of a construction due to Van Nypelseer, Beiträge Algebra Geom. 46 (2005), no. 2, 561–574. MR MR2196938

The residually weakly primitive geometries of \( HS \), Australas. J. Combin. 33 (2005), 231–236. MR MR2170360


Real and Complex Geometry
51Mxx


General Convexity
52Axx

Polytopes and Polyhedra

52Bxx


Differential Geometry

53Xxx


Group Theory
Permutation Groups
20Bxx


[86] Markus Kirschmer, Finite symplectic matrix groups.


[128] William F. Reynolds, *Noncommutators and the number of projective characters of a finite group*, The Arcata Conference on Representations of Finite Groups (Arcata,


Abstract Finite Groups
20Dxx


[52] _____; *The poset of elementary abelian \( p \)-subgroups having rank at least 2*, J. Group. Th (To appear).


164


[147] Colin Reid, A problem in the Kourovka notebook concerning the number of conjugacy classes of a finite group, 2008.


Ivan Yudin, *Presentation for parabolic subgroups of GL_n(F_2)*, 2010.
Structure and Classification
20Exx


Special Aspects of Finite or Infinite Groups

20Fxx


[90] Ivan Marin and Jean Michel, \textit{Automorphisms of complex reflection groups}, 2007.


[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.


Linear Algebraic Groups


[56] [Author], 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


Cohomology
20Jxx


Loops, Quasigroups and Semigroups
20Mxx, 20Nxx


[34] ______, *Computing with root subgroups of twisted reductive groups*, 2009.


[65] George Havas and Edmund F. Robertson, *Application of computational tools for finitely presented groups*, Computational support for discrete mathematics (Piscat-


K-Theory

All Areas

19Xxx


Linear Algebra
Linear Algebra and Matrices

15-xx


Computational Linear Algebra


[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


Number Theory

Elementary Number Theory

11Axx except 11A41 and 11A51, 11Cxx


Primality and Factorisation
11A41, 11A51


Sequences and Sets

11Bxx


Diophantine Equations

11Dxx


David Brown, *Primitive integral solutions to* $x^2 + y^3 = z^{10}$, 2009.


Discontinuous Groups and Automorphic Forms
11Fxx


[27] Lassina Dembele, Matthew Greenberg, and John Voight, Nonsolvable number fields ramified only at 3 and 5, 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.


238


Arithmetic Algebraic Geometry
11Gxx


[34] Antoine Chambert-Loir, *Compter (rapidement) le nombre de solutions d’équations dans les corps finis*, 2006.


[61] Lassina Dembele, Matthew Greenberg, and John Voight, *Nonsolvable number fields ramified only at 3 and 5*, 2009.


[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


[121] ———, *On symmetric square values of quadratic polynomials*, 2010.


253


[166] Dominic Lanphier, The trace of special values of modular \(L\)-functions.


[186] Ekin Ozman, *Local points on quadratic twists of \(X_0(N)\)*, 2009.


Geometry of Numbers
11Hxx


263

Zeta and $L$-functions: Analytic Theory

11Mxx


Algebraic Number Theory
11Rxx and 11Sxx


[70] Piotr Maciak, *Primes of the form $x^2 + n \ast y^2$ in function fields*, 2009.


[73] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group \( c2 \times c2 \times c2 \)*, Journal of Number Theory *129* (2009), no. 1, 231–245.


Finite Fields
11Txx


[21] Dae San Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, 2008.


Computational Methods
11-04 and 11Yxx


[34] Nils Bruin and Michael Stoll, Two-cover descent on hyperelliptic curves, 2008.


[38] ______, Fast point counting on genus two curves in characteristic three, 2010.


[106] Michael Monagan and Mark van Hoeij, *A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions*.


[111] Harris Nover, *Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group $c2 \times c2 \times c2$*, Journal of Number Theory 129 (2009), no. 1, 231 – 245.


[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.

Numerical Analysis
All Areas
65Xxx


Probability and Statistics

Probability

60Xxx


Topological and Lie Groups

Lie Groups

22Exx


Noncompact Transformation Groups


Algebraic Topology
55Xxx, 55Rxx, 55Sxx


Homology Theory

55Nxx, 55Pxx, 55Qxx


Spectral Sequences
55Txx


Low-dimensional Topology
57Mxx


Topological Manifolds
57Nxx


Coding Theory

Linear Codes: General

94B05, 94B12, 94B60


[42] Dae San Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, 2008.


314


Cyclic Codes
94B15


Self-Dual Codes


[64] Hyun Kwang Kim, Dae Kyu Kim, and Jon-Lark Kim, *Type I codes over GF(4)*, Ars Combin. To appear.


Algebraic Geometry Codes
94B27, 94B40


Combinatorial Codes

94B25


[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)


[36] J. D. Key and M. J. de Resmini, Small sets of even type and codewords, J. Geom. 61

95 (2001), no. 1-2, 229–236, Special issue on design combinatorics: in honor of S. S.

[38] J. D. Key, T. P. McDonough, and V. C. Mavron, Information sets and partial permuta-
tion decoding for codes from finite geometries, Finite Fields Appl. 12 (2006), no. 2,


[40] J. D. Key and J. Moori, Some irreducible codes invariant under the Janko group, J1
or J2, 2008.

[41] J. D. Key, J. Moori, and B. G. Rodrigues, On some designs and codes from primitive


[43] ______, Permutation decoding for the binary codes from triangular graphs, European


[45] ______, Partial permutation decoding of some binary codes from graphs on triples,
Ars Combin. 91 (2009), 363–371. MR MR2501975


Codes over Galois Rings


Low-Density Parity Check Codes


Lattice Codes
94B10


Quantum Error-Correcting Codes

See also Quantum Computation


Computational Methods


Artificial Intelligence
68Txx


Symbolic and Computational Algebra

68W30


Cryptography

Cryptography: General


Block Ciphers


Stream Ciphers


Public Key Cryptography
See also Curve-Based Public Key Cryptography


365


368


Curve-Based Cryptography


Protocols


Random Number Generators


Computational Methods


Information and Communication

Information
94Axx except 94A60, 94A62


385
Circuits and Networks

94Cxx


Signal Processing


Data Mining

Biology
Mathematical Biology
92Bxx


Mathematical Programming
90Cxx


Physics
Mechanics
70Fxx


Quantum Theory
81Xxx except 81P68


Quantum Computation
81P68


[17] Michel Planat, Peter Levay, and Metod Saniga, Balanced tripartite entanglement, the alternating group A4 and the Lie algebra sl(3,c) ⊕ u(1), 2009.


Relativity and Gravitation


