A Selection of Books, Papers, and Theses
Citing Magma

Computational Algebra Group
University of Sydney

April 14, 2023
Contents

Overview of the Bibliography 1
  Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
  Citing Magma in Publications . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1
  Bibliography Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
  Acknowledgements . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

Publications Citing Magma 4
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(ii) Most unpublished papers unless they are stored in the arXiv.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.
Publications Citing Magma


[374] Charles Bouillaguet, Pierre-Alain Fouque1, Antoine Joux, and Joana Treger, A family of weak keys in HFE (and the corresponding practical key-recovery), pp. 1–16.


[380] Irene I. Bouw and Brian Osserman, Some 4-point Hurwitz numbers in positive characteristic, 2009.


S. Allen Broughton, *Enumeration of the equisymmetric strata of the moduli space of surfaces of low genus*.


[452] ———, *Primitive integral solutions to $x^2 + y^3 = z^10$*, 2009.


[521] Stanislav Bulygin and Michael Brickenstein, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, 2008.


[639] Bill Casselman, Computation in Coxeter groups. II. Constructing minimal roots, Represent. Theory 12 (2008), 260–293. MR2439007


Constructing symmetric graphs, Theta 3 (1989), 11–16.


Antonio Cossidente and Sam K. J. Vereecke, *Some geometry of the isomorphism* Sp(4,q) ∼= O(5,q), q even, J. Geom. 70 (2001), no. 1-2, 28–37. MR MR1825542 (2002g:05043)


85


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


87


[975] ———, Index calculus in class groups of plane curves of small degree, 2005.


[977] 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


[979] 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.


[983] 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)


[1138] Winfried Fakler, *Algorithmen zur symbolischen lösung homogener linearer differen-


[1141] Xin Gui Fang, George Havas, and Jie Wang, *Automorphism groups of certain non-


[1155] Rene P. Felix, The finite quotient groups of the plane crystallographic group $p6m$, Matimyás Mat. (1989), no. 1, 39–49. MR MR1040006 (90m:20054)


105


108

[1190] [1191] [1192] [1193] [1194] [1195] [1196] [1197] [1198] [1199] [1200] [1201]


[1428] Grigor Grigorov, Andrei Jorza, Stephan Patrikis, William A. Stein, and Corina Tar-


[1433] Fritz Grunewald and Alexander Lubotzky, *Linear representations of the automor-


[1435] Jordi Guàrdia, *Jacobian Nullwerte, periods and symmetric equations for hyper-

[1436] Jordi Guardia, Jesus Montes, and Enric Nart, *Higher Newton polygons in the com-

129


[1494] Brian Hansen, *Explicit computations supporting a generalization of Serre’s conjecture*, MSc, Brigham Young University, 2005.


[1497] Jill Hanson and Michael J. Kallaher, *Finite Bol quasifields are nearfields*, Utilitas Math. **37** (1990), 45–64. MR MR1068509 (92b:51024)


136


[1636] 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


[1638] 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

[1639] 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.


149


[1670] Stephen P. Humphries and Zane Kun Li, *Counting powers of words in monoids*, European J. Combin. 30 (2009), no. 5, 1297–1308. MR MR2514653


[1808] ______, Partial permutation decoding of some binary codes from graphs on triples, Ars Combin. 91 (2009), 363–371. MR MR2501975


[1848] Dae San Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, 2008.


[1870] Markus Kirschmer, Finite symplectic matrix groups.


167


[2034] Wolfgang Lempken, Two new symmetric 2-(144,66,30) designs.


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


[2232] Michael Monagan and Mark van Hoeij, A modular algorithm for computing polynomial GCDs over number fields presented with multiple extensions.


[2319] 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.


207


[2377] Sebastian Pauli and Florence Soriano-Gafiuk, *The discrete logarithm in logarithmic $l$-class groups and its applications in $K$-theory*, Algorithmic Number Theory,


[2402] Francesco Dalla Piazza and Bert van Geemen, Siegel modular forms and finite symplectic groups, 2008.


[2411] , Entangling gates in even Euclidean lattices such as Leech lattice, 2010.


[2414] Michel Planat, Peter Levay, and Metod Saniga, Balanced tripartite entanglement, the alternating group $A_4$ and the Lie algebra sl(3,c) ⊕ u(1), 2009.


[2426] ______, *On maximal finite irreducible subgroups of GL$(n, \mathbb{Z})$. 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)


On equations of double planes with $p_g = q = 1$, Math. Comp 79 (2010), 1091–1108.


Daniel Robbins, Broue’s abelian defect group conjecture for the Tits group, 2008.


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.


[2612] 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.


233


[2717] M. Chiara Tamburini and M. Vsemirnov, Irreducible $(2, 3, 7)$-subgroups of $\text{PGL}_n(F)$, $n \leq 7$, J. Algebra 300 (2006), no. 1, 339–362. MR MR2228652


[2817] 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


[2896] Ivan Yudin, *Presentation for parabolic subgroups of GL_n(F_2)*, 2010.

253


