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(ii) Most unpublished papers unless they are stored in the arXiv.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


19


[184] M. Barbosa, R. Noad, D. Page, and N. P. Smart, *First steps toward a cryptography-aware language and compiler*.


[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.


[562] Jason Todd Callahan, The arithmetic and geometry of two-generator Kleinian groups, Phd, University of Texas at Austin, 2009.


[621] ———, The poset of elementary abelian p-subgroups having rank at least 2, J. Group. Th (To appear).


72


Willem A. de Graaf and Andrea Pavan, *Constructing arithmetic subgroups of unipotent groups*, J. Algebra **322** (2009), no. 11, 3950–3970. MR MR2556132


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-


[1186] 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


[1482] Emmanuel Hallouin, *Study and computation of a Hurwitz space and totally real 
$\mathrm{PSL}_2(F_8)$-extensions of $\mathbb{Q}$*, J. Algebra **292** (2005), no. 1, 259–281. MR MR2166804 (2006h:14041)


[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)


1671] Stephen P. Humphries and Zane Kun Li, Counting powers of words in monoids, European J. Combin. 30 (2009), no. 5, 1297–1308. MR MR2514653


152


[1724] Antoine Joux, Reynald Lercier, David Naccache, and Emmanuel Thomé, Oracle-assisted static Diffie-Hellman is easier than discrete logarithms, 2008.


154


[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.


Jürgen Klüners and Sebastian Pauli, *Computing residue class rings and Picard groups of orders*, J. Algebra **292** (2005), no. 1, 47–64. MR MR2166795


[1917] 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 2489254


171


R. V. Kravchenko and B. V. Petrenko, Some formulas for the minimal number of generators of the direct sum of matrix rings, 2007.


Wolfgang Lempken, Two new symmetric 2-\( (144,66,30) \) designs.


196


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


204


[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.


[2333] Cryptanalysis of the birational permutation signature scheme over a non-commutative ring, 2009.


209


Christopher Parker, Sporadic simple groups which are completions of the Goldschmidt $G_3$-amalgam, J. Algebra **235** (2001), no. 1, 131–153. MR MR1807659 (2001k:20030)


Christopher Parker, 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)


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


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


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


[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.


[2809] ———, *On the $(2,3)$-generation of matrix groups over the ring of integers*, Algebra i Analiz **19** (2007), no. 6, 22–58. MR MR2411638


[2889] Dan Yasaki, Binary Hermitian forms over a cyclotomic field, J. Algebra 322 (2009), no. 11, 4132–4142. MR MR2556143


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


Fangguo Zhang, *Twisted ate pairing on hyperelliptic curves and applications*, 2008.


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.


