A Selection of Books, Papers, and Theses
Citing Magma

Computational Algebra Group
University of Sydney

June 4, 2020
## Contents

<table>
<thead>
<tr>
<th>Overview of the Bibliography</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Citing Magma in Publications</td>
<td>1</td>
</tr>
<tr>
<td>Bibliography Files</td>
<td>2</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>2</td>
</tr>
</tbody>
</table>

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(ii) Most unpublished papers unless they are stored in the arXiv.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


[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.


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


[663] ______, *On the equation s\textsuperscript{2} + y\textsuperscript{2p} = α\textsuperscript{3}*, Math. Comp. **77** (2008), no. 262, 1223–1227. MR MR2373199


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


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


Solving the Diophantine equation \( y^2 = x(x^2 - n^2) \), J. Number Theory 129 (2009), no. 1, 102–121. MR MR2468473 (2009j:11047)


104


[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)


[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


113


[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)


[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.


[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


[1773] ____, 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

[1774] ____, An algorithm to calculate optimal homogeneous systems of parameters, J.

[1775] ____, The depth of invariant rings and cohomology, J. Algebra 245 (2001), no. 2,

[1776] ____, The calculation of radical ideals in positive characteristic, J. Symbolic Com-

[1777] ____, Computing invariants of reductive groups in positive characteristic, Trans-

[1778] ____, The computation of invariant fields and a constructive version of a theo-
(2008m:13011)

[1779] 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)

[1780] Gregor Kemper and Gunter Malle, Invariant fields of finite irreducible reflection

[1781] Gregor Kemper and Allan Steel, Some algorithms in invariant theory of finite
groups, Computational Methods for Representations of Groups and Algebras (Essen,
(2000j:13009)

Soc. 28 (1983), no. 1, 131–133. MR MR726809 (85a:20014)

[1783] ____, Efficient presentations for three simple groups, Comm. Algebra 14 (1986),
no. 5, 797–800. MR MR834464 (87c:20060)

[1784] ____, Some new efficient soluble groups, Comm. Algebra 18 (1990), no. 8, 2747–
2753. MR MR1074253 (91j:20081)


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


1821  Jennifer D. Key and Johannes Siemons, *Closure properties of the special linear groups*, Ars Combin. **22** (1986), 107–117. MR MR867739 (88a:20009)


[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.


[1974]  

[1975]  


[2033] ______, The structure of the projective indecomposable modules of $\hat{3}M_{22}$ in characteristic 2, Math. Comp. 62 (1994), no. 206, 841–850. MR MR1216260 (94g:20016)

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


(2130) 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


192


[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.


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


212


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


———, *Decomposing symmetric powers of certain modular representations of cyclic groups*, Progress in Mathematics **278** (2010), 169–196.


[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.


[2632] [2632], Character degrees and derived length in p-groups, Glasgow Math. J. 30 (1988), no. 2, 221–230. MR MR942995 (89g:20017)


[2634] [2634], Generation of groups of square-free order, J. Symbolic Comput. 42 (2007), no. 6, 668–677. MR MR2325920


[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


[2874] 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.


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


