Journal of Symbolic Computation, Volume 31
Numbers 1 and 2

Special Issue on Computational Algebra and Number Theory: Proceedings of the Second Magma Conference

FOREWORD .................................................................................................................. 1
von zur Gathen, J. and Panario, D., Factoring Polynomials Over Finite Fields: A Survey ........................................... 3
Gao, S., On the Deterministic Complexity of Factoring Polynomials ................................................................. 19
Key, J. D., Some Applications of Magma in Designs and Codes: Oval Designs, Hermitian Unitals and Generalized Reed–Muller Codes ................................................................. 37
Ebert, G. L., Constructions in Finite Geometry Using Computer Algebra Systems ...................................................... 55
Cremona, J. E., Classical Invariants and 2-descent on Elliptic Curves .................................................................. 71
Buhler, J., Crandall, R., Ernvall, R., Metsänkylä, T. and Shokrollahi, M. A., Irregular Primes and Cyclotomic Invariants to 12 Million .............................................................................. 89
Bosma, W. and de Smit, B., Class Number Relations from a Computational Point of View ................................. 97
Daberkow, M., On Computations in Kummer Extensions ........................................................................ 113
Cohen, H., Diaz y Diaz, F. and Olivier, M., Algorithmic Methods for Finitely Generated Abelian Groups ........................................... 133
Cannon, J. J., Cox, B. C. and Holt, D. F., Computing the Subgroups of a Permutation Group ........................................ 149
Lux, K. and Wiegelmann, M., Determination of Socle Series using the Condensation Method ........................ 163
Slattery, M. C., Computing Double Cosets in Soluble Groups ........................................................................ 179
Norton, S., Computing in the Monster ............................................................................................................ 193
Gollan, H. W., A New Existence Proof for $L_9$, the Sporadic Simple Group of R. Lyons ................................. 203
Griess Jr., R. L. and Ryba, A. J. E., Embeddings of $PSL(2,41)$ and $PSL(2,49)$ in $E_6(C)$ ........................................ 211
Carlson, J. F., Calculating Group Cohomology: Tests for Completion ................................................................. 229
Sausse, A., A New Approach to Primary Decomposition ......................................................................................... 243
Koppenhagen, U. and Mayr, E. W., An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals, and Applications to Commutative Semigroups ................................. 259
## Number 3

Baader, F. and Narendran, P., Unification of Concept Terms in Description Logics ........................................... 277
Kalorkoti, K., Counting and Gröbner Bases ........................................... 307
Lickteig, T. and Roy, M.-F., Sylvester–Habicht Sequences and Fast Cauchy Index Computation ........................................... 315
Orecchia, F., Implicitization of a General Union of Parametric Varieties ........................................... 343

## Number 4

Aries, F. and Senoussi, R., An Implicitization Algorithm for Rational Surfaces with no Base Points ........................................... 357
Howlett, R. B., Rylands, L. J. and Taylor, D. E., Matrix Generators for Exceptional Groups of Lie Type ........................................... 429
Mulders, T., A Generalized Sylvester Identity and Fraction-free Random Gaussian Elimination ........................................... 447

### Applications

Khanin, R. and Cartmell, M., Parallelization of Perturbation Analysis: Application to Large-scale Engineering Problems ........................................... 461
Merlet, J.-P., A Parser for the Interval Evaluation of Analytical Functions and its Application to Engineering Problems ........................................... 475

## Number 5

Ayari, A. and Basin, D., A Higher-order Interpretation of Deductive Tableau ........................................... 487
Brown, C. W., Simple CAD Construction and its Applications ........................................... 521
Brueggeman, S., Septic Number Fields Which are Ramified Only at One Small Prime ........................................... 549
Burckel, S., Syntactical Methods for Braids of Three Strands ........................................... 557
Byrne, E. and Fitzpatrick, P., Gröbner Bases over Galois Rings with an Application to Decoding Alternant Codes ........................................... 565
D’Andrea, C., Resultants and Moving Surfaces ........................................... 585
Shaska, T., Curves of Genus 2 with $(N, N)$ Decomposable Jacobians ........................................... 603
Zheng, J. and Sederberg, T. W., A Direct Approach to Computing the $\mu$-basis of Planar Rational Curves ........................................... 619
## CONTENTS

### Number 6

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bouziane, D., Rody, A. K. and Maârouf, H., Unmixed-dimensional De-</td>
<td>631</td>
</tr>
<tr>
<td>composition of a Finitely Generated Perfect Differential Ideal</td>
<td></td>
</tr>
<tr>
<td>Chionh, E.-W., Rectangular Corner Cutting and Dixon $A$-resultants</td>
<td>651</td>
</tr>
<tr>
<td>Kalorkoti, K., Detecting Algebraic Curves in Bad Position</td>
<td>671</td>
</tr>
<tr>
<td>Li, Z. and Schwarz, F., Rational Solutions of Riccati-like Partial</td>
<td>691</td>
</tr>
<tr>
<td>Differential Equations</td>
<td></td>
</tr>
<tr>
<td>van der Hoeven, J., Fast Evaluation of Holonomic Functions Near and</td>
<td>717</td>
</tr>
<tr>
<td>in Regular Singularities</td>
<td></td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td></td>
</tr>
<tr>
<td>Bebbington, D. and Göbel, M., <strong>KLEIN</strong>: a <em>MATHEMATICA</em> Package for</td>
<td>745</td>
</tr>
<tr>
<td>Radar Polarimetry Based on Spinor and Tensor Algebra</td>
<td></td>
</tr>
</tbody>
</table>
Index to Volume 31

Algorithmic Methods for Finitely Generated Abelian Groups, 133

Aries, F. and Senoussi, R., An Implicitization Algorithm for Rational Surfaces with no Base Points, 357

Ayari, A. and Basin, D., A Higher-order Interpretation of Deductive Tableau, 487

Baader, F. and Narendran, P., Unification of Concept Terms in Description Logics, 277

Bebbington, D. and Göbel, M., Klein: a Mathematica Package for Radar Polarimetry Based on Spinor and Tensor Algebra, 745

Bosma, W. and de Smit, B., Class Number Relations from a Computational Point of View, 97

Bouziane, D., Rody, A. K. and Maaroufi, H., Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal, 631

Brown, C. W., Simple CAD Construction and its Applications, 521

Brueggeman, S., Septic Number Fields Which are Ramified Only at One Small Prime, 549

Buhler, J., Crandall, R., Ernvall, R., Metsänkylä, T. and Shokrollahi, M. A., Irregular Primes and Cyclotomic Invariants to 12 Million, 89

Burckel, S., Syntactical Methods for Braids of Three Strands, 557

Byrne, E. and Fitzpatrick, P., Gröbner Bases over Galois Rings with an Application to Decoding Alternant Codes, 565

Calculating Group Cohomology: Tests for Completion, 229

Cannon, J. J., Cox, B. C. and Holt, D. F., Computing the Subgroups of a Permutation Group, 149

Carlson, J. F., Calculating Group Cohomology: Tests for Completion, 229

Chionh, E.-W., Rectangular Corner Cutting and Dixon A-resultants, 651

Chromium, E.-W., Classical Invariants and 2-descent on Elliptic Curves, 71

Class Number Relations from a Computational Point of View, 97

Cremona, J. E., Classical Invariants and 2-descent on Elliptic Curves, 71

Cohen, H., Diaz y Diaz, F. and Olivier, M., Algorithmic Methods for Finitely Generated Abelian Groups, 133

Computing Double Cosets in Soluble Groups, 179

Computing in the Monster, 193

Computing the Subgroups of a Permutation Group, 149

Constructions in Finite Geometry Using Computer Algebra Systems, 55

Counting and Gröbner Bases, 307

Cremona, J. E., Classical Invariants and 2-descent on Elliptic Curves, 71

Curves of Genus 2 with (N, N) Decomposable Jacobians, 603

D'Andrea, C., Resultants and Moving Surfaces, 585

Daberkow, M., On Computations in Kummer Extensions, 113
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decomposition Plans for Geometric Constraint Systems, Part I: Performance Measures for CAD</td>
<td>367</td>
</tr>
<tr>
<td>Decomposition Plans for Geometric Constraint Problems, Part II: New Algorithms</td>
<td>409</td>
</tr>
<tr>
<td>Detecting Algebraic Curves in Bad Position</td>
<td>671</td>
</tr>
<tr>
<td>Determination of Socle Series using the Condensation Method</td>
<td>163</td>
</tr>
<tr>
<td>A Direct Approach to Computing the $\mu$-basis of Planar Rational Curves</td>
<td>619</td>
</tr>
<tr>
<td>Ebert, G. L., Constructions in Finite Geometry Using Computer Algebra Systems</td>
<td>55</td>
</tr>
<tr>
<td>Embeddings of $PSL(2,41)$ and $PSL(2,49)$ in $E_8(C)$</td>
<td>211</td>
</tr>
<tr>
<td>Factoring Polynomials Over Finite Fields: A Survey</td>
<td>3</td>
</tr>
<tr>
<td>Fast Evaluation of Holonomic Functions Near and in Regular Singularities</td>
<td>717</td>
</tr>
<tr>
<td>Gao, S., On the Deterministic Complexity of Factoring Polynomials</td>
<td>19</td>
</tr>
<tr>
<td>von zur Gathen, J. and Panario, D., Factoring Polynomials Over Finite Fields: A Survey</td>
<td>3</td>
</tr>
<tr>
<td>A Generalized Sylvester Identity and Fraction-free Random Gaussian Elimination</td>
<td>447</td>
</tr>
<tr>
<td>Gollan, H. W., A New Existence Proof for $Ly$, the Sporadic Simple Group of R. Lyons</td>
<td>203</td>
</tr>
<tr>
<td>Gries Jr., R. L. and Ryba, A. J., Embeddings of $PSL(2,41)$ and $PSL(2,49)$ in $E_8(C)$</td>
<td>211</td>
</tr>
<tr>
<td>Gröbner Bases over Galois Rings with an Application to Decoding Alternant Codes</td>
<td>565</td>
</tr>
<tr>
<td>A Higher-order Interpretation of Deductive Tableau</td>
<td>487</td>
</tr>
<tr>
<td>van der Hoeven, J., Fast Evaluation of Holonomic Functions Near and in Regular Singularities</td>
<td>717</td>
</tr>
<tr>
<td>Howlett, R. B., Rylands, L. J. and Taylor, D. E., Matrix Generators for Exceptional Groups of Lie Type</td>
<td>429</td>
</tr>
<tr>
<td>An Implicitization Algorithm for Rational Surfaces with no Base Points</td>
<td>357</td>
</tr>
<tr>
<td>Implicitization of a General Union of Parametric Varieties</td>
<td>343</td>
</tr>
<tr>
<td>Irregular Primes and Cyclotomic Invariants to 12 Million</td>
<td>89</td>
</tr>
<tr>
<td>Klein: a Mathematica Package for Radar Polarimetry Based on Spinor and Tensor Algebra</td>
<td>745</td>
</tr>
</tbody>
</table>
Index to Volume 31

Kalorkoti, K., Counting and Gröbner Bases, 307
Kalorkoti, K., Detecting Algebraic Curves in Bad Position, 671
Key, J. D., Some Applications of Magma in Designs and Codes: Oval Designs, Hermitian Unitals and Generalized Reed–Muller Codes, 37
Khanin, R. and Carmell, M., Parallelization of Perturbation Analysis: Application to Large-scale Engineering Problems, 461
Koppenhagen, U. and Mayer, E. W., An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals, and Applications to Commutative Semigroups, 259

Li, Z. and Schwarz, F., Rational Solutions of Riccati-like Partial Differential Equations, 691
Lickteig, T. and Roy, M.-F., Sylvester–Habicht Sequences and Fast Cauchy Index Computation, 315
Lux, K. and Wiegelmann, M., Determination of Socle Series using the Condensation Method, 163

Matrix Generators for Exceptional Groups of Lie Type, 429
Merlet, J.-P., A Parser for the Interval Evaluation of Analytical Functions and its Application to Engineering Problems, 475
Mulders, T., A Generalized Sylvester Identity and Fraction-free Random Gaussian Elimination, 447

A New Approach to Primary Decomposition, 243
A New Existence Proof for Ly, the Sporadic Simple Group of R. Lyons, 203
Norton, S., Computing in the Monster, 193

On Computations in Kummer Extensions, 113
On the Deterministic Complexity of Factoring Polynomials, 19
An Optimal Algorithm for Constructing the Reduced Gröbner Basis of Binomial Ideals, and Applications to Commutative Semigroups, 259
Orecchia, F., Implicitization of a General Union of Parametric Varieties, 343

Parallelization of Perturbation Analysis: Application to Large-scale Engineering Problems, 461
A Parser for the Interval Evaluation of Analytical Functions and its Application to Engineering Problems, 475

Rational Solutions of Riccati-like Partial Differential Equations, 691
Rectangular Corner Cutting and Dixon A-resultants, 651
Resultants and Moving Surfaces, 585

Sausse, A., A New Approach to Primary Decomposition, 243
Septic Number Fields Which are Ramified Only at One Small Prime, 549
SHASKA, T., Curves of Genus 2 with \((N,N)\) Decomposable Jacobians, 603
Simple CAD Construction and its Applications, 521
SLATTERY, M. C., Computing Double Cosets in Soluble Groups, 179
Some Applications of Magma in Designs and Codes: Oval Designs, Hermitian
Unifats and Generalized Reed–Muller Codes, 37
Special Issue on Computational Algebra and Number Theory: Proceedings of the
Second Magma Conference—Foreword, 1
Sylvester–Habicht Sequences and Fast Cauchy Index Computation, 315
Syntactical Methods for Braids of Three Strands, 557

Unification of Concept Terms in Description Logics, 277
Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential
Ideal, 631

ZHENG, J. and SEDERBERG, T. W., A Direct Approach to Computing the
\(\mu\)-basis of Planar Rational Curves, 619