
VOLUME 73 NUMBER 248



OCTOBER 2004

MATHEMATICS OF COMPUTATION

A M E R I C A N M A T H E M A T I C A L S O C I E T Y

EDITED BY

Randolph E. Bank
Christine Bernardi
Peter B. Borwein
David W. Boyd
Susanne C. Brenner
Richard P. Brent
Carsten Carstensen
Arjeh M. Cohen
Ronald F. A. Cools
Howard Elman
Richard S. Falk
Daniel W. Lozier
Zhi-Quan Luo
Harald Niederreiter
Ricardo H. Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Igor E. Shparlinski
Chi-Wang Shu, *Managing Editor*
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin
Joseph D. Ward
Hugh C. Williams
Jinchao Xu

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Available electronically at
www.ams.org/mcom/

Mathematics of Computation

This journal is devoted to research articles of the highest quality in computational mathematics. Areas covered include numerical analysis, computational discrete mathematics, including number theory, algebra and combinatorics, and related fields such as stochastic numerical methods. Articles must be of significant computational interest and contain original and substantial mathematical analysis or development of computational methodology. Reviews of books in areas related to computational mathematics are also included.

Submission information. See **Information for Authors** at the end of this issue.

Publisher Item Identifier. The Publisher Item Identifier (PII) appears at the top of the first page of each article published in this journal. This alphanumeric string of characters uniquely identifies each article and can be used for future cataloging, searching, and electronic retrieval.

Postings to the AMS website. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

Subscription information. *Mathematics of Computation* is published quarterly. Beginning in January 1996 *Mathematics of Computation* is accessible from www.ams.org/journals/. Subscription prices for Volume 73 (2004) are as follows: for paper delivery, \$436 list, \$349 institutional member, \$392 corporate member, \$283 member of CBMS organizations; \$262 individual member; for electronic delivery, \$392 list, \$314 institutional member, \$353 corporate member, \$255 member of CBMS organizations, \$235 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add \$15 for surface delivery outside the United States and India; \$18 to India. Expedited delivery to destinations in North America is \$17; elsewhere \$56.

Back number information. For back issues see the www.ams.org/bookstore.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904 USA. *All orders must be accompanied by payment.* Other correspondence should be addressed to 201 Charles Street, Providence, RI 02904-2294 USA.

Copying and reprinting. Material in this journal may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

Mathematics of Computation is published quarterly by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2294 USA. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

© 2004 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index®*, *Science Citation Index™-Expanded*, *ISI Alerting ServicesSM*, *CompuMath Citation Index®*, and *Current Contents®/Physical, Chemical & Earth Sciences*.

⊗ The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability.

MATHEMATICS OF COMPUTATION
CONTENTS

Vol. 73, No. 248

October 2004

Nicolas Neuss and Christian Wieners, Criteria for the approximation property for multigrid methods in nonnested spaces	1583
I. Babuška and S. A. Sauter, Algebraic algorithms for the analysis of mechanical trusses	1601
Alan Demlow, Localized pointwise error estimates for mixed finite element methods	1623
Huo-Yuan Duan and Guo-Ping Liang, A locking-free Reissner-Mindlin quadrilateral element	1655
M. Amara, E. Chacón Vera, and D. Trujillo, Vorticity-velocity-pressure formulation for Stokes problem	1673
Maxim A. Olshanskii and Arnold Reusken, Grad-div stablilization for Stokes equations	1699
J. L. Guermond and Jie Shen, On the error estimates for the rotational pressure-correction projection methods	1719
James H. Bramble and Joseph E. Pasciak, A new approximation technique for div-curl systems	1739
Paola Pozzi, L^2 -estimate for the discrete Plateau Problem	1763
Xavier Antoine, Christophe Besse, and Vincent Mouysset, Numerical schemes for the simulation of the two-dimensional Schrödinger equation using non-reflecting boundary conditions	1779
I. Alonso-Mallo, B. Cano, and J. C. Jorge, Spectral-fractional step Runge–Kutta discretizations for initial boundary value problems with time dependent boundary conditions	1801
Xiaobai Sun and Enrique S. Quintana-Ortí, Spectral division methods for block generalized Schur decompositions	1827
Marcelo Queiroz, Joaquim Júdice, and Carlos Humes, Jr., The symmetric eigenvalue complementarity problem	1849
Jerry Eriksson and Mårten E. Gulliksson, Local results for the Gauss–Newton method on constrained rank-deficient nonlinear least squares	1865
Fred J. Hickernell, Ian H. Sloan, and Grzegorz W. Wasilkowski, On tractability of weighted integration over bounded and unbounded regions in \mathbb{R}^s	1885
Fred J. Hickernell, Ian H. Sloan, and Grzegorz W. Wasilkowski, On strong tractability of weighted multivariate integration	1903
Bin Han, Thomas P.-Y. Yu, and Bruce Piper, Multivariate refinable Hermite interpolant	1913
Iván Area, Dimitar K. Dimitrov, Eduardo Godoy, and André Ronveaux, Zeros of Gegenbauer and Hermite polynomials and connection coefficients	1937
Christian Lécot and Wolfgang Wagner, A quasi–Monte Carlo scheme for Smoluchowski’s coagulation equation	1953
J. Dick and F. Y. Kuo, Reducing the construction cost of the component-by-component construction of good lattice rules	1967
Ichiro Shimada, Rational double points on supersingular $K3$ surfaces	1989

Arthur Baragar , Canonical vector heights on K3 surfaces with Picard number three—An argument for nonexistence	2019
Neal Koblitz and Alfred J. Menezes , Obstacles to the torsion-subgroup attack on the decision Diffie-Hellman Problem	2027
Pilar Fernandez-Ferreiros and M. Angeles Gomez-Molleda , Deciding the nilpotency of the Galois group by computing elements in the centre	2043
Karim Belabas , On quadratic fields with large 3-rank	2061
Petteri Kaski and Patric R. J. Östergård , The Steiner triple systems of order 19	2075
Garikai Campbell , Points on $y = x^2$ at rational distance	2093
G. J. van der Heiden , Addendum to “Factoring polynomials over finite fields with Drinfeld modules”	2109
Reviews and Descriptions of Tables and Books	2111
Klaus Höllig 9, C. T. Kelley 10	

INDEX TO VOLUME 73 (2004)

- Aguirre, Julián, Castañeda, Fernando, and Peral, Juan Carlos. *High rank elliptic curves with torsion group $\mathbb{Z}/(2\mathbb{Z})$* , 323
- Ahn, Jaehyun. *See Bae, Sunghan*
- Akrisis, Georgios, and Crouzeix, Michel. *Linearly implicit methods for nonlinear parabolic equations*, 613
- Allombert, Bill. *An efficient algorithm for the computation of Galois automorphisms*, 359
- Alonso-Mallo, I., Cano, B., and Jorge, J. C. *Spectral-fractional step Runge–Kutta discretizations for initial boundary value problems with time dependent boundary conditions*, 1801
- Alonso-Mallo, Isaías, and Reguera, Nuria. *Discrete absorbing boundary conditions for Schrödinger-type equations. Practical implementation*, 127
- Amara, M., Chacón Vera, E., and Trujillo, D. *Vorticity-velocity-pressure formulation for Stokes problem*, 1673
- Antoine, Xavier, Besse, Christophe, and Mouysset, Vincent. *Numerical schemes for the simulation of the two-dimensional Schrödinger equation using non-reflecting boundary conditions*, 1779
- Area, Iván, Dimitrov, Dimitar K., Godoy, Eduardo, and Ronveaux, André. *Zeros of Gegenbauer and Hermite polynomials and connection coefficients*, 1937
- Aregba-Driollet, D., Natalini, R., and Tang, S. *Explicit diffusive kinetic schemes for nonlinear degenerate parabolic systems*, 63
- Asai, Nobuyoshi. *See Miyazaki, Yoshinori*
- Atkin, A. O. L., and Bernstein, D. J. *Prime sieves using binary quadratic forms*, 1023
- Axler, Sheldon, Gorkin, Pamela, and Voss, Karl. *The Dirichlet problem on quadratic surfaces*, 637
- Babuška, I., and Sauter, S. A. *Algebraic algorithms for the analysis of mechanical trusses*, 1601
- Bae, Sunghan, Jung, Hwanyup, and Ahn, Jaehyun. *Class numbers of some abelian extensions of rational function fields*, 377
- Baragar, Arthur. *Canonical vector heights on K3 surfaces with Picard number three—An argument for nonexistence*, 2019
- Barnett, A. Ross. *See Broughan, Kevin A.*
- Bauer, Mark L. *The arithmetic of certain cubic function fields*, 387
- Belabas, Karim. *On quadratic fields with large 3-rank*, 2061
- Bernstein, D. J. *See Atkin, A. O. L.*
- Berrizbeitia, Pedro, and Berry, T. G. *Biquadratic reciprocity and a Lucasian primality test*, 1559
- Berry, T. G. *See Berrizbeitia, Pedro*
- Bertoluzza, Silvia. *Substructuring preconditioners for the three fields domain decomposition method*, 659
- Besse, Christophe. *See Antoine, Xavier*
- Bobenko, Alexander. *See Deconinck, Bernard*
- Borwein, P. B., and Ferguson, R. A. *A complete description of Golay pairs for lengths up to 100*, 967
- Bossy, Mireille. *Optimal rate of convergence of a stochastic particle method to solutions of 1D viscous scalar conservation laws*, 777
- Bramble, James H., and Pasciak, Joseph E. *A new approximation technique for div-curl systems*, 1739
- Brenner, Susanne C. *Convergence of nonconforming V-cycle and F-cycle multigrid algorithms for second order elliptic boundary value problems*, 1041
_____. *Korn's inequalities for piecewise H^1 vector fields*, 1067
- Breuning, Manuel. *On equivariant global epsilon constants for certain dihedral extensions*, 881
- Broughan, Kevin A., and Barnett, A. Ross. *The holomorphic flow of the Riemann zeta function*, 987
- Browkin, Jerzy. *Some new kinds of pseudoprimes*, 1031
- Bruin, Nils. *Visualising Sha[2] in Abelian surfaces*, 1459
- Cai, DongSheng. *See Miyazaki, Yoshinori*
- Campbell, Garikai. *Points on $y = x^2$ at rational distance*, 2093
- Cannon, John R. *See El-Gamel, Mohamed*
- Cano, B. *See Alonso-Mallo, I.*
- Carstensen, C. *All first-order averaging techniques for a posteriori finite element error control on unstructured grids are efficient and reliable*, 1153

- Castañeda, Fernando. *See* Aguirre, Julián
- Chacón Vera, E. *See* Amara, M.
- Chen, Imin, and Cummins, Chris. *Elliptic curves with nonsplit mod 11 representations*, 869
- Chen, Zhiming, and Feng, Jia. *An adaptive finite element algorithm with reliable and efficient error control for linear parabolic problems*, 1167
- Christiansen, Snorre H. *Discrete Fredholm properties and convergence estimates for the electric field integral equation*, 143
- Climent, Joan-Josep, Perea, Carmen, Tortosa, Leandro, and Zamora, Antonio. *Sequential and parallel synchronous alternating iterative methods*, 691
- Cockburn, Bernardo, Kanschat, Guido, and Schötzau, Dominik. *The local discontinuous Galerkin method for the Oseen equations*, 569
- Cohen, Arjeh M., Murray, Scott H., and Taylor, D. E. *Computing in groups of Lie type*, 1477
- Conflitti, Alessandro, and Shparlinski, Igor E. *On the multidimensional distribution of the subset sum generator of pseudorandom numbers*, 1005
- Criscuolo, G. *A note on a paper by G. Mastroianni and G. Monegato*, 243
- Crouzeix, Michel. *See* Akrivis, Georgios
- Cummins, Chris. *See* Chen, Imin
- Dahmen, W., Faermann, B., Graham, I. G., Hackbusch, W., and Sauter, S. A. *Inverse inequalities on non-quasi-uniform meshes and application to the mortar element method*, 1107
- Damelin, S. B. *Asymptotics of recurrence coefficients for orthonormal polynomials on the line—Magnus's method revisited*, 191
- Datskovsky, B., and Guerzhoy, P. *Searching for Kummer congruences in an infinite slope family*, 861
- Deconinck, Bernard, Heil, Matthias, Bobenko, Alexander, van Hoeij, Mark, and Schmies, Marcus. *Computing Riemann theta functions*, 1417
- Deléglise, Marc, Dusart, Pierre, and Roblot, Xavier-François. *Counting primes in residue classes*, 1565
- Demlow, Alan. *Piecewise linear finite element methods are not localized*, 1195
- _____. *Localized pointwise error estimates for mixed finite element methods*, 1623
- Despres, Bruno. *Lax theorem and finite volume schemes*, 1203
- Dick, J., and Kuo, F. Y. *Reducing the construction cost of the component-by-component construction of good lattice rules*, 1967
- Dimitrov, Dimitar K. *See* Area, Iván
- Dryanov, D. P., Qazi, M. A., and Rahman, Q. I. *Local behaviour of polynomials*, 1345
- Duan, Huo-Yuan, and Liang, Guo-Ping. *Nonconforming elements in least-squares mixed finite element methods*, 1
- _____. *A locking-free Reissner-Mindlin quadrilateral element*, 1655
- Dummit, David S., Tangedal, Brett A., and van Wamelen, Paul B. *Stark's conjecture over complex cubic number fields*, 1525
- Dusart, Pierre. *See* Deléglise, Marc
- El-Gamel, Mohamed, Cannon, John R., and Zayed, Ahmed I. *Sinc-Galerkin method for solving linear sixth-order boundary-value problems*, 1325
- Eriksson, Jerry, and Gulliksson, Mårten E. *Local results for the Gauss-Newton method on constrained rank-deficient nonlinear least squares*, 1865
- Faermann, B. *See* Dahmen, W.
- Fang, Kai-Tai, and Ge, Gennian. *A sensitive algorithm for detecting the inequivalence of Hadamard matrices*, 843
- Feng, Jia. *See* Chen, Zhiming
- Feng, Xiaobing, and Prohl, Andreas. *Analysis of a fully discrete finite element method for the phase field model and approximation of its sharp interface limits*, 541
- Ferguson, R. A. *See* Borwein, P. B.
- Fernandez-Ferreiros, Pilar, and Gomez-Molleda, M. Angeles. *Deciding the nilpotency of the Galois group by computing elements in the centre*, 2043
- Filaseta, Michael, and Schinzel, Andrzej. *On testing the divisibility of lacunary polynomials by cyclotomic polynomials*, 957
- Gajda, Piotr, Li, Youming, Plaskota, Leszek, and Wasilkowski, Grzegorz W. *A Monte Carlo algorithm for weighted integration over \mathbb{R}^d* , 813
- von zur Gathen, Joachim, and Nöcker, Michael. *Computing special powers in finite fields*, 1499

INDEX TO VOLUME 73 (2004)

- Gavrilyuk, Ivan P., Hackbusch, Wolfgang, and Khoromskij, Boris N. *Data-sparse approximation to the operator-valued functions of elliptic operator*, 1297
- Ge, Gennian. *See Fang, Kai-Tai*
- George, Alan, and Ikramov, Khakim D. *Gaussian elimination is stable for the inverse of a diagonally dominant matrix*, 653
- Godoy, Eduardo. *See Area, Iván*
- Gomez-Molleda, M. Angeles. *See Fernandez-Ferreiros, Pilar*
- Gorkin, Pamela. *See Axler, Sheldon*
- Goto, T., and Shibata, S. *All numbers whose positive divisors have integral harmonic mean up to 300*, 475
- Graham, I. G. *See Dahmen, W.*
- Greither, Cornelius, Roblot, Xavier-François, and Tangedal, Brett A. *The Brumer-Stark conjecture in some families of extensions of specified degree*, 297
- Groenewegen, Richard P. *Bounds for computing the tame kernel*, 1443
- Guermoud, J. L., and Shen, Jie. *On the error estimates for the rotational pressure-correction projection methods*, 1719
- Guerzhoy, P. *See Datskovsky, B.*
- Guessab, Allal, and Schmeisser, Gerhard. *Convexity results and sharp error estimates in approximate multivariate integration*, 1365
- Gulliksson, Mårten E. *See Eriksson, Jerry*
- Guo, Ben-yu, and Xu, Cheng-long. *Mixed Laguerre-Legendre pseudospectral method for incompressible fluid flow in an infinite strip*, 95
- Hackbusch, W. *See Dahmen, W.*
- Hackbusch, Wolfgang. *See Gavrilyuk, Ivan P.*
- Han, Bin, Yu, Thomas P.-Y., and Piper, Bruce. *Multivariate refinable Hermite interpolant*, 1913
- van der Heiden, G. J. *Factoring polynomials over finite fields with Drinfeld modules*, 317
- _____. *Addendum to “Factoring polynomials over finite fields with Drinfeld modules”*, 2109
- Heil, Matthias. *See Deconinck, Bernard*
- Heinrich, Stefan, Hickernell, Fred J., and Yue, Rong-Xian. *Optimal quadrature for Haar wavelet spaces*, 259
- Hickernell, Fred J. *See Heinrich, Stefan*
- Hickernell, Fred J., Sloan, Ian H., and Wasilkowski, Grzegorz W. *On tractability of weighted integration over bounded and unbounded regions in \mathbb{R}^s* , 1885
- _____. *On strong tractability of weighted multivariate integration*, 1903
- van Hoeij, Mark. *See Deconinck, Bernard*
- Holden, Joshua. *First-hit analysis of algorithms for computing quadratic irregularity*, 939
- Hu, Qiyi, and Zou, Jun. *Substructuring preconditioners for saddle-point problems arising from Maxwell's equations in three dimensions*, 35
- Huang, Jianguo. *Numerical solution of the elastic body-plate problem by nonoverlapping domain decomposition type techniques*, 19
- Huang, Yunqing, Shi, Zhongci, Tang, Tao, and Xue, Weimin. *A multilevel successive iteration method for nonlinear elliptic problems*, 525
- Humes, Carlos, Jr. *See Queiroz, Marcelo*
- Ikebe, Yasuhiko. *See Miyazaki, Yoshinori*
- Ikramov, Khakim D. *See George, Alan*
- Jorge, J. C. *See Alonso-Mallo, I.*
- Júdice, Joaquim. *See Queiroz, Marcelo*
- Jung, Hwanyup. *See Bae, Sunghan*
- Kanschat, Guido. *See Cockburn, Bernardo*
- Karlsen, K. H., Klingenberg, C., and Risebro, N. H. *A relaxation scheme for conservation laws with a discontinuous coefficient*, 1235
- Kaski, Petteri, and Östergård, Patric R. J. *The Steiner triple systems of order 19*, 2075
- Khoromskij, Boris N. *See Gavrilyuk, Ivan P.*
- Khuri-Makdisi, Kamal. *Linear algebra algorithms for divisors on an algebraic curve*, 333
- Kikuchi, Yasushi. *See Miyazaki, Yoshinori*
- Klingenberg, C. *See Karlsen, K. H.*
- Koblitz, Neal, and Menezes, Alfred J. *Obstacles to the torsion-subgroup attack on the decision Diffie-Hellman Problem*, 2027

INDEX TO VOLUME 73 (2004)

- Kotnik, Tadej. *Computational estimation of the order of $\zeta(\frac{1}{2} + it)$* , 949
 Kuo, F. Y. *See Dick, J.*
 Kvernadze, George. *Approximating the jump discontinuities of a function by its Fourier-Jacobi coefficients*, 731
 Lazebnik, Felix, and Thomason, Andrew. *Orthomorphisms and the construction of projective planes*, 1547
 Lécot, Christian, and Wagner, Wolfgang. *A quasi-Monte Carlo scheme for Smoluchowski's coagulation equation*, 1953
 Li, Youming. *See Gajda, Piotr*
 Liang, Guo-Ping. *See Duan, Huo-Yuan*
 Lyness, J. N., and Sørevik, T. *Four-dimensional lattice rules generated by skew-circulant matrices*, 279
 Mathé, Peter, and Wei, Gang. *Quasi-Monte Carlo integration over \mathbb{R}^d* , 827
 McLaughlin, Philip B., Jr. *New frameworks for Montgomery's modular multiplication method*, 899
 Menezes, Alfred J. *See Koblitz, Neal*
 Miyazaki, Yoshinori, Asai, Nobuyoshi, Kikuchi, Yasushi, Cai, DongSheng, and Ikebe, Yasuhiko. *Computation of multiple eigenvalues of infinite tridiagonal matrices*, 719
 Montgomery, Hugh L., and Vorhauer, Ulrike M. A. *Greedy sums of distinct squares*, 493
 Moore, Gerald. *Laguerre approximation of stable manifolds with application to connecting orbits*, 211
 Mora, Carlos M. *Numerical simulation of stochastic evolution equations associated to quantum Markov semigroups*, 1393
 Moree, Pieter. *Chebyshev's bias for composite numbers with restricted prime divisors*, 425
 Moree, Pieter, and te Riele, Herman J. J. *The hexagonal versus the square lattice*, 451
 Mouysset, Vincent. *See Antoine, Xavier*
 Murray, Scott H. *See Cohen, Arjeh M.*
 Natalini, R. *See Aregba-Driollet, D.*
 Neuss, Nicolas, and Wieners, Christian. *Criteria for the approximation property for multigrid methods in nonnested spaces*, 1583
 Nievergelt, Yves. *Perturbation analysis for circles, spheres, and generalized hyperspheres fitted to data by geometric total least-squares*, 169
 Nöcker, Michael. *See von zur Gathen, Joachim*
 Olshanskii, Maxim A., and Reusken, Arnold. *Grad-div stabilization for Stokes equations*, 1699
 Östergård, Patric R. J. *See Kaski, Petteri*
 Pasciak, Joseph E. *See Bramble, James H.*
 Peña, J. M. *A stable test to check if a matrix is a nonsingular M-matrix*, 1385
 Peral, Juan Carlos. *See Aguirre, Julián*
 Perea, Carmen. *See Climent, Joan-Josep*
 Pillichshammer, Friedrich. *A lower bound for rank 2 lattice rules*, 853
 Piper, Bruce. *See Han, Bin*
 Plaskota, Leszek. *See Gajda, Piotr*
 Pozzi, Paola. *L^2 -estimate for the discrete Plateau Problem*, 1763
 Prohl, Andreas. *See Feng, Xiaobing*
 Qazi, M. A. *See Dryanov, D. P.*
 Queiroz, Marcelo, Júdice, Joaquim, and Humes, Carlos, Jr. *The symmetric eigenvalue complementarity problem*, 1849
 Quintana-Ortí, Enrique S. *See Sun, Xiaobai*
 Rahman, Q. I. *See Dryanov, D. P.*
 Reguera, Nuria. *See Alonso-Mallo, Isaías*
 Reusken, Arnold. *See Olshanskii, Maxim A.*
 te Riele, Herman J. J. *See Moree, Pieter*
 Risebro, N. H. *See Karlsen, K. H.*
 Roblot, Xavier-François. *See Deléglise, Marc*
 _____. *See Greither, Cornelius*
 Ronveaux, André. *See Area, Iván*
 Sauer, Thomas. *Lagrange interpolation on subgrids of tensor product grids*, 181
 Sauter, S. A. *See Babuška, I.*

- _____. *See* Dahmen, W.
- Schatz, Alfred H., and Wahlbin, Lars B. *Asymptotically exact a posteriori estimators for the pointwise gradient error on each element in irregular meshes. Part II: The piecewise linear case*, 517
- Schinzel, Andrzej. *See* Filaseta, Michael
- Schmeisser, Gerhard. *See* Guessab, Allal
- Schmies, Marcus. *See* Deconinck, Bernard
- Schötzau, Dominik. *See* Cockburn, Bernardo
- Shen, Jie. *See* Guermond, J. L.
- Shi, Zhongci. *See* Huang, Yunqing
- Shibata, S. *See* Goto, T.
- Shimada, Ichiro. *Rational double points on supersingular K3 surfaces*, 1989
- Shparlinski, Igor E. *See* Conflitti, Alessandro
- Sloan, Ian H. *See* Hickernell, Fred J.
- Sørevik, T. *See* Lyness, J. N.
- Spotz, William F. *See* Swarztrauber, Paul N.
- Sun, Xiaobai, and Quintana-Ortí, Enrique S. *Spectral division methods for block generalized Schur decompositions*, 1827
- Suzuki, Koji. *An estimate for the number of integers without large prime factors*, 1013
- Swarztrauber, Paul N., and Spotz, William F. *Spherical harmonic projectors*, 753
- Tang, S. *See* Aregba-Driollet, D.
- Tang, Tao. *See* Huang, Yunqing
- Tangedal, Brett A. *See* Dummit, David S.
_____. *See* Greither, Cornelius
- Taylor, D. E. *See* Cohen, Arjeh M.
- Thomason, Andrew. *See* Lazebnik, Felix
- Tortosa, Leandro. *See* Climent, Joan-Josep
- Trujillo, D. *See* Amara, M.
- Tsumura, Hirofumi. *Evaluation formulas for Tornheim's type of alternating double series*, 251
- Vorhauer, Ulrike M. A. *See* Montgomery, Hugh L.
- Voss, Karl. *See* Axler, Sheldon
- Wagner, Wolfgang. *See* Lécot, Christian
- Wahlbin, Lars B. *See* Schatz, Alfred H.
- van Wamelen, Paul B. *See* Dummit, David S.
- Wasilkowski, Grzegorz W. *See* Gajda, Piotr
_____. *See* Hickernell, Fred J.
- Watkins, Mark. *Real zeros of real odd Dirichlet L-functions*, 415
- _____. *Class numbers of imaginary quadratic fields*, 907
- Wei, Gang. *See* Mathé, Peter
- Wieners, Christian. *See* Neuss, Nicolas
- Xu, Cheng-long. *See* Guo, Ben-yu
- Xu, Jinchao, and Zhang, Zhimin. *Analysis of recovery type a posteriori error estimators for mildly structured grids*, 1139
- Xue, Weimin. *See* Huang, Yunqing
- Ye, Mao. *Existence and asymptotic stability of relaxation discrete shock profiles*, 1261
- Ying, Lung-An. *Finite difference method for a combustion model*, 595
- Yu, Thomas P.-Y. *See* Han, Bin
- Yue, Rong-Xian. *See* Heinrich, Stefan
- Zamora, Antonio. *See* Climent, Joan-Josep
- Zanna, Antonella. *Recurrence relations and convergence theory of the generalized polar decomposition on Lie groups*, 761
- Zayed, Ahmed I. *See* El-Gamel, Mohamed
- Zhang, Zhimin. *See* Xu, Jinchao
- Zhao, Jun. *Analysis of finite element approximation for time-dependent Maxwell problems*, 1089
- Zou, Jun. *See* Hu, Qiya

INDEX OF REVIEWS BY AUTHOR OF WORK REVIEWED

<i>Author</i>	<i>Review Number</i>	<i>Classification</i>	<i>Page</i>
BEN-TAL, AHARON, & NEMIROVSKI, ARKADI	3	90C25, 90C05	1040
BUHMANN, M. D.	6	41-02, 41A63, 41A30, 41A05, 65-02	1578
DEVILLE, M. O., FISCHER, P. F., & MUND, E. H.	2	65M70, 76D05	1039
FEDKIW, RON	5	See OSHER, STANLEY	1578
FISCHER, P. F.	2	See DEVILLE, M. O.	1039
HANDSCOMB, D. C.	4	See MASON, J. C.	1577
HÖLLIG, KLAUS	9	65N30, 65N50, 65N15	2111
KELLEY, C. T.	10	65H05, 65H10, 65F10, 65F22	2113
MASON, J. C., & HANDSCOMB, D. C.	4	33C45	1577
MOLLIN, R. A.	8	94A60, 11T71, 11Y16	1582
MUND, E. H.	2	See DEVILLE, M. O.	1039
NEMIROVSKI, ARKADI	3	See BEN-TAL, AHARON	1040
OSHER, STANLEY, & FEDKIW, RON	5	65Mxx, 65C20, 65Dxx, 65-02, 76-xx	1578
RENEGAR, JAMES	1	90C25, 90C51	515
SHPARLINSKI, I.	7	11K45, 11T71, 11Yxx, 68Q17, 94-02	1581

INDEX OF REVIEWS BY SUBJECT OF WORK REVIEWED

<i>Author</i>	<i>Review Number</i>	<i>Title</i>	<i>Page</i>
11-XX Number theory			
11K45 <i>Pseudo-random numbers; Monte Carlo methods</i>			
SHPARLINSKI, I.	7	Cryptographic applications of analytic number theory	1581
11T71 <i>Algebraic coding theory; cryptography</i>			
MOLLIN, R. A.	8	RSA and public-key cryptography	1582
SHPARLINSKI, I.	7	Cryptographic applications of analytic number theory	1581
11Yxx <i>Computational number theory</i>			
SHPARLINSKI, I.	7	Cryptographic applications of analytic number theory	1581
11Y16 <i>Algorithms; complexity</i>			
MOLLIN, R. A.	8	RSA and public-key cryptography	1582
33-XX Special functions			
33C45 <i>Orthogonal polynomials and functions of hypergeometric type (Jacobi, Laguerre, Hermite, Askey scheme, etc.)</i>			
MASON, J. C., & HANDSCOMB, D. C.	4	Chebyshev polynomials	1577

INDEX OF REVIEWS BY SUBJECT OF WORK REVIEWED

41-XX Approximations and expansions

41-02 *Research exposition (monographs, survey articles)*

BUHMANN, M. D.	6	Radial basis functions: theory and implementations	1578
41A05 <i>Interpolation</i>			
BUHMANN, M. D.	6	Radial basis functions: theory and implementations	1578
41A30 <i>Approximation by other special function classes</i>			
BUHMANN, M. D.	6	Radial basis functions: theory and implementations	1578
41A63 <i>Multidimensional problems (should also be assigned at least one other classification number in this section)</i>			
BUHMANN, M. D.	6	Radial basis functions: theory and implementations	1578

65-XX Numerical analysis

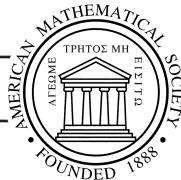
65-02 *Research exposition (monographs, survey articles)*

BUHMANN, M. D.	6	Radial basis functions: theory and implementations	1578
OSHER, STANLEY, & FEDKIW, RON	5	Level set methods and dynamic implicit surfaces	1578
65C20 <i>Models, numerical methods</i>			
OSHER, STANLEY, & FEDKIW, RON	5	Level set methods and dynamic implicit surfaces	1578
65Dxx <i>Numerical approximation and computational geometry (primarily algorithms)</i>			
OSHER, STANLEY, & FEDKIW, RON	5	Level set methods and dynamic implicit surfaces	1578
65F10 <i>Iterative methods for linear systems</i>			
KELLEY, C. T.	10	Solving nonlinear equations with Newton's method	2113
65F22 <i>Ill-posedness, regularization</i>			
KELLEY, C. T.	10	Solving nonlinear equations with Newton's method	2113
65H05 <i>Single equations</i>			
KELLEY, C. T.	10	Solving nonlinear equations with Newton's method	2113
65H10 <i>Systems of equations</i>			
KELLEY, C. T.	10	Solving nonlinear equations with Newton's method	2113
65Mxx <i>Partial differential equations, initial value and time-dependent initial-boundary value problems</i>			
OSHER, STANLEY, & FEDKIW, RON	5	Level set methods and dynamic implicit surfaces	1578
65M70 <i>Spectral, collocation and related methods</i>			
DEVILLE, M. O., FISCHER, P. F., & MUND, E. H.	2	High-order methods for incompressible fluid flow	1039

INDEX OF REVIEWS BY SUBJECT OF WORK REVIEWED

65N15	<i>Error bounds</i>		
HÖLLIG, KLAUS	9	Finite element methods and B-splines	2111
65N30	<i>Finite elements, Rayleigh-Ritz and Galerkin methods, finite methods</i>		
HÖLLIG, KLAUS	9	Finite element methods and B-splines	2111
65N50	<i>Mesh generation and refinement</i>		
HÖLLIG, KLAUS	9	Finite element methods and B-splines	2111
68-XX Computer science			
68Q17	<i>Computational difficulty of problems (lower bounds, completeness, difficulty of approximation, etc.)</i>		
SHPARLINSKI, I.	7	Cryptographic applications of analytic number theory	1581
76-XX Fluid mechanics			
76-xx	<i>Fluid mechanics</i>		
OSHER, STANLEY, & FEDKIW, RON	5	Level set methods and dynamic implicit surfaces	1578
76D05	<i>Navier-Stokes equations</i>		
DEVILLE, M. O., FISCHER, P. F., & MUND, E. H.	2	High-order methods for incompressible fluid flow	1039
90-XX Operations research, mathematical programming			
90C05	<i>Linear programming</i>		
BEN-TAL, AHARON, & NEMIROVSKI, ARKADI	3	Lectures on modern convex optimization: analysis, algorithms and engineering applications	1040
90C25	<i>Convex programming</i>		
BEN-TAL, AHARON, & NEMIROVSKI, ARKADI	3	Lectures on modern convex optimization: analysis, algorithms and engineering applications	1040
RENEGAR, JAMES	1	A mathematical view of interior-point methods in convex optimization	515
90C51	<i>Interior-point methods</i>		
RENEGAR, JAMES	1	A mathematical view of interior-point methods in convex optimization	515
94-XX Information and communication, circuits			
94-02	<i>Research exposition (monographs, survey articles)</i>		
SHPARLINSKI, I.	7	Cryptographic applications of analytic number theory	1581
94A60	<i>Cryptography</i>		
MOLLIN, R. A.	8	RSA and public-key cryptography	1582

VOLUME 73



2004

MATHEMATICS OF COMPUTATION

A M E R I C A N M A T H E M A T I C A L S O C I E T Y

EDITED BY

Randolph E. Bank
Christine Bernardi
Peter B. Borwein
David W. Boyd
Susanne C. Brenner
Richard P. Brent
Carsten Carstensen
Arjeh M. Cohen
Ronald F. A. Cools
Howard Elman
Richard S. Falk
Daniel W. Lozier
Zhi-Quan Luo
Harald Niederreiter
Ricardo H. Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Igor E. Shparlinski
Chi-Wang Shu, *Managing Editor*
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin
Joseph D. Ward
Hugh C. Williams
Jinchao Xu

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Mathematics of Computation

This journal is devoted to research articles of the highest quality in computational mathematics. Areas covered include numerical analysis, computational discrete mathematics, including number theory, algebra and combinatorics, and related fields such as stochastic numerical methods. Articles must be of significant computational interest and contain original and substantial mathematical analysis or development of computational methodology. Reviews of books in areas related to computational mathematics are also included.

Submission information. See **Information for Authors** at the end of this issue.

Publisher Item Identifier. The Publisher Item Identifier (PII) appears at the top of the first page of each article published in this journal. This alphanumeric string of characters uniquely identifies each article and can be used for future cataloging, searching, and electronic retrieval.

Postings to the AMS website. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

Subscription information. *Mathematics of Computation* is published quarterly. Beginning in January 1996 *Mathematics of Computation* is accessible from www.ams.org/journals/. Subscription prices for Volume 73 (2004) are as follows: for paper delivery, \$436 list, \$349 institutional member, \$392 corporate member, \$283 member of CBMS organizations; \$262 individual member; for electronic delivery, \$392 list, \$314 institutional member, \$353 corporate member, \$255 member of CBMS organizations, \$235 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add \$15 for surface delivery outside the United States and India; \$18 to India. Expedited delivery to destinations in North America is \$17; elsewhere \$56.

Back number information. For back issues see the www.ams.org/bookstore.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904 USA. *All orders must be accompanied by payment.* Other correspondence should be addressed to 201 Charles Street, Providence, RI 02904-2294 USA.

Copying and reprinting. Material in this journal may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. Requests can also be made by e-mail to reprint-permission@ams.org.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

Mathematics of Computation is published quarterly by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2294 USA. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

© 2004 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index®*, *Science Citation Index™-Expanded*, *ISI Alerting ServicesSM*, *CompuMath Citation Index®*, and *Current Contents®/Physical, Chemical & Earth Sciences*.

⊗ The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability.

MATHEMATICS OF COMPUTATION
CONTENTS

Vol. 73, No. 245

January 2004

Huo-Yuan Duan and Guo-Ping Liang, Nonconforming elements in least-squares mixed finite element methods	1
Jianguo Huang, Numerical solution of the elastic body-plate problem by nonoverlapping domain decomposition type techniques	19
Qiya Hu and Jun Zou, Substructuring preconditioners for saddle-point problems arising from Maxwell's equations in three dimensions	35
D. Aregba-Drollet, R. Natalini, and S. Tang, Explicit diffusive kinetic schemes for nonlinear degenerate parabolic systems	63
Ben-yu Guo and Cheng-long Xu, Mixed Laguerre-Legendre pseudospectral method for incompressible fluid flow in an infinite strip	95
Isaías Alonso-Mallo and Nuria Reguera, Discrete absorbing boundary conditions for Schrödinger-type equations. Practical implementation ..	127
Snorre H. Christiansen, Discrete Fredholm properties and convergence estimates for the electric field integral equation	143
Yves Nievergelt, Perturbation analysis for circles, spheres, and generalized hyperspheres fitted to data by geometric total least-squares	169
Thomas Sauer, Lagrange interpolation on subgrids of tensor product grids	181
S. B. Damelin, Asymptotics of recurrence coefficients for orthonormal polynomials on the line—Magnus's method revisited	191
Gerald Moore, Laguerre approximation of stable manifolds with application to connecting orbits	211
G. Criscuolo, A note on a paper by G. Mastroianni and G. Monegato ..	243
Hirofumi Tsumura, Evaluation formulas for Tornheim's type of alternating double series	251
Stefan Heinrich, Fred J. Hickernell, and Rong-Xian Yue, Optimal quadrature for Haar wavelet spaces	259
J. N. Lyness and T. Sørevik, Four-dimensional lattice rules generated by skew-circulant matrices	279
Cornelius Greither, Xavier-François Roblot, and Brett A. Tangedal, The Brumer-Stark conjecture in some families of extensions of specified degree	297
G. J. van der Heiden, Factoring polynomials over finite fields with Drinfeld modules	317
Julián Aguirre, Fernando Castañeda, and Juan Carlos Peral, High rank elliptic curves with torsion group $\mathbb{Z}/(2\mathbb{Z})$	323
Kamal Khuri-Makdisi, Linear algebra algorithms for divisors on an algebraic curve	333
Bill Allombert, An efficient algorithm for the computation of Galois automorphisms	359
Sunghan Bae, Hwanyup Jung, and Jaehyun Ahn, Class numbers of some abelian extensions of rational function fields	377
Mark L. Bauer, The arithmetic of certain cubic function fields	387
Mark Watkins, Real zeros of real odd Dirichlet L -functions	415

Pieter Moree , Chebyshev's bias for composite numbers with restricted prime divisors	425
Pieter Moree and Herman J.J. te Riele , The hexagonal versus the square lattice	451
T. Goto and S. Shibata , All numbers whose positive divisors have integral harmonic mean up to 300	475
Hugh L. Montgomery and Ulrike M. A. Vorhauer , Greedy sums of distinct squares	493
Reviews and Descriptions of Tables and Books	515
James Renegar 1	

Vol. 73, No. 246

April 2004

Alfred H. Schatz and Lars B. Wahlbin , Asymptotically exact a posteriori estimators for the pointwise gradient error on each element in irregular meshes. Part II: The piecewise linear case	517
Yunqing Huang, Zhongci Shi, Tao Tang, and Weimin Xue , A multilevel successive iteration method for nonlinear elliptic problems	525
Xiaobing Feng and Andreas Prohl , Analysis of a fully discrete finite element method for the phase field model and approximation of its sharp interface limits	541
Bernardo Cockburn, Guido Kanschat, and Dominik Schötzau , The local discontinuous Galerkin method for the Oseen equations	569
Lung-An Ying , Finite difference method for a combustion model	595
Georgios Akrivis and Michel Crouzeix , Linearly implicit methods for nonlinear parabolic equations	613
Sheldon Axler, Pamela Gorkin, and Karl Voss , The Dirichlet problem on quadratic surfaces	637
Alan George and Khakim D. Ikramov , Gaussian elimination is stable for the inverse of a diagonally dominant matrix	653
Silvia Bertoluzza , Substructuring preconditioners for the three fields domain decomposition method	659
Joan-Josep Climent, Carmen Perea, Leandro Tortosa, and Antonio Zamora , Sequential and parallel synchronous alternating iterative methods	691
Yoshinori Miyazaki, Nobuyoshi Asai, Yasushi Kikuchi, DongSheng Cai, and Yasuhiko Ikebe , Computation of multiple eigenvalues of infinite tridiagonal matrices	719
George Kvernadze , Approximating the jump discontinuities of a function by its Fourier-Jacobi coefficients	731
Paul N. Swarztrauber and William F. Spotz , Spherical harmonic projectors	753
Antonella Zanna , Recurrence relations and convergence theory of the generalized polar decomposition on Lie groups	761

Mireille Bossy, Optimal rate of convergence of a stochastic particle method to solutions of 1D viscous scalar conservation laws	777
Piotr Gajda, Youming Li, Leszek Plaskota, and Grzegorz W. Wasilkowski, A Monte Carlo algorithm for weighted integration over \mathbb{R}^d	813
Peter Mathé and Gang Wei, Quasi-Monte Carlo integration over \mathbb{R}^d ...	827
Kai-Tai Fang and Gennian Ge, A sensitive algorithm for detecting the inequivalence of Hadamard matrices	843
Friedrich Pillichshammer, A lower bound for rank 2 lattice rules	853
B. Datskovsky and P. Guerzhoy, Searching for Kummer congruences in an infinite slope family	861
Imin Chen and Chris Cummins, Elliptic curves with nonsplit mod 11 representations	869
Manuel Breuning, On equivariant global epsilon constants for certain dihedral extensions	881
Philip B. McLaughlin, Jr., New frameworks for Montgomery's modular multiplication method	899
Mark Watkins, Class numbers of imaginary quadratic fields	907
Joshua Holden, First-hit analysis of algorithms for computing quadratic irregularity	939
Tadej Kotnik, Computational estimation of the order of $\zeta(\frac{1}{2} + it)$	949
Michael Filaseta and Andrzej Schinzel, On testing the divisibility of lacunary polynomials by cyclotomic polynomials	957
P. B. Borwein and R. A. Ferguson, A complete description of Golay pairs for lengths up to 100	967
Kevin A. Broughan and A. Ross Barnett, The holomorphic flow of the Riemann zeta function	987
Alessandro Conflitti and Igor E. Shparlinski, On the multidimensional distribution of the subset sum generator of pseudorandom numbers ...	1005
Koji Suzuki, An estimate for the number of integers without large prime factors	1013
A. O. L. Atkin and D. J. Bernstein, Prime sieves using binary quadratic forms	1023
Jerzy Browkin, Some new kinds of pseudoprimes	1031
Reviews and Descriptions of Tables and Books	1039
M. O. Deville, P. F. Fischer, and E. H. Mund 2 , Aharon Ben-Tal and Arkadi Nemirovski 3	

Susanne C. Brenner, Convergence of nonconforming V-cycle and F-cycle multigrid algorithms for second order elliptic boundary value problems 1041	
Susanne C. Brenner, Korn's inequalities for piecewise H^1 vector fields .. 1067	
Jun Zhao, Analysis of finite element approximation for time-dependent Maxwell problems	1089

W. Dahmen, B. Faermann, I. G. Graham, W. Hackbusch, and S. A. Sauter, Inverse inequalities on non-quasi-uniform meshes and application to the mortar element method	1107
Jinchao Xu and Zhimin Zhang, Analysis of recovery type a posteriori error estimators for mildly structured grids	1139
C. Carstensen, All first-order averaging techniques for a posteriori finite element error control on unstructured grids are efficient and reliable ..	1153
Zhiming Chen and Jia Feng, An adaptive finite element algorithm with reliable and efficient error control for linear parabolic problems	1167
Alan Demlow, Piecewise linear finite element methods are not localized ..	1195
Bruno Despres, Lax theorem and finite volume schemes	1203
K. H. Karlsen, C. Klingenberg, and N. H. Risebro, A relaxation scheme for conservation laws with a discontinuous coefficient	1235
Mao Ye, Existence and asymptotic stability of relaxation discrete shock profiles	1261
Ivan P. Gavrilyuk, Wolfgang Hackbusch, and Boris N. Khoromskij, Data-sparse approximation to the operator-valued functions of elliptic operator	1297
Mohamed El-Gamel, John R. Cannon, and Ahmed I. Zayed, Sinc-Galerkin method for solving linear sixth-order boundary-value problems	1325
D. P. Dryanov, M. A. Qazi, and Q. I. Rahman, Local behaviour of polynomials	1345
Allal Guessab and Gerhard Schmeisser, Convexity results and sharp error estimates in approximate multivariate integration	1365
J. M. Peña, A stable test to check if a matrix is a nonsingular M-matrix ..	1385
Carlos M. Mora, Numerical simulation of stochastic evolution equations associated to quantum Markov semigroups	1393
Bernard Deconinck, Matthias Heil, Alexander Bobenko, Mark van Hoeij, and Marcus Schmies, Computing Riemann theta functions	1417
Richard P. Groenewegen, Bounds for computing the tame kernel	1443
Nils Bruin, Visualising Sha[2] in Abelian surfaces	1459
Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, Computing in groups of Lie type	1477
Joachim von zur Gathen and Michael Nöcker, Computing special powers in finite fields	1499
David S. Dummit, Brett A. Tangedal, and Paul B. van Wamelen, Stark's conjecture over complex cubic number fields	1525
Felix Lazebnik and Andrew Thomason, Orthomorphisms and the construction of projective planes	1547
Pedro Berrizbeitia and T. G. Berry, Biquadratic reciprocity and a Lucasian primality test	1559
Marc Deléglise, Pierre Dusart, and Xavier-François Roblot, Counting primes in residue classes	1565
Reviews and Descriptions of Tables and Books	1577
J. C. Mason and D. C. Handscomb 4, Stanley Osher and Ron Fedkiw 5, M. D. Buhmann 6, I. Shparlinski 7, R. A. Mollin 8	

Nicolas Neuss and Christian Wieners, Criteria for the approximation property for multigrid methods in nonnested spaces	1583
I. Babuška and S. A. Sauter, Algebraic algorithms for the analysis of mechanical trusses	1601
Alan Demlow, Localized pointwise error estimates for mixed finite element methods	1623
Huo-Yuan Duan and Guo-Ping Liang, A locking-free Reissner-Mindlin quadrilateral element	1655
M. Amara, E. Chacón Vera, and D. Trujillo, Vorticity-velocity-pressure formulation for Stokes problem	1673
Maxim A. Olshanskii and Arnold Reusken, Grad-div stablilization for Stokes equations	1699
J. L. Guermond and Jie Shen, On the error estimates for the rotational pressure-correction projection methods	1719
James H. Bramble and Joseph E. Pasciak, A new approximation technique for div-curl systems	1739
Paola Pozzi, L^2 -estimate for the discrete Plateau Problem	1763
Xavier Antoine, Christophe Besse, and Vincent Mouysset, Numerical schemes for the simulation of the two-dimensional Schrödinger equation using non-reflecting boundary conditions	1779
I. Alonso-Mallo, B. Cano, and J. C. Jorge, Spectral-fractional step Runge-Kutta discretizations for initial boundary value problems with time dependent boundary conditions	1801
Xiaobai Sun and Enrique S. Quintana-Ortí, Spectral division methods for block generalized Schur decompositions	1827
Marcelo Queiroz, Joaquim Júdice, and Carlos Humes, Jr., The symmetric eigenvalue complementarity problem	1849
Jerry Eriksson and Mårten E. Gulliksson, Local results for the Gauss-Newton method on constrained rank-deficient nonlinear least squares ..	1865
Fred J. Hickernell, Ian H. Sloan, and Grzegorz W. Wasilkowski, On tractability of weighted integration over bounded and unbounded regions in \mathbb{R}^s	1885
Fred J. Hickernell, Ian H. Sloan, and Grzegorz W. Wasilkowski, On strong tractability of weighted multivariate integration	1903
Bin Han, Thomas P.-Y. Yu, and Bruce Piper, Multivariate refinable Hermite interpolant	1913
Iván Area, Dimitar K. Dimitrov, Eduardo Godoy, and André Ronveaux, Zeros of Gegenbauer and Hermite polynomials and connection coefficients	1937
Christian Lécot and Wolfgang Wagner, A quasi-Monte Carlo scheme for Smoluchowski's coagulation equation	1953
J. Dick and F. Y. Kuo, Reducing the construction cost of the component-by-component construction of good lattice rules	1967
Ichiro Shimada, Rational double points on supersingular $K3$ surfaces	1989
Arthur Baragar, Canonical vector heights on $K3$ surfaces with Picard number three—An argument for nonexistence	2019

Neal Koblitz and Alfred J. Menezes, Obstacles to the torsion-subgroup attack on the decision Diffie-Hellman Problem	2027
Pilar Fernandez-Ferreiros and M. Angeles Gomez-Molleda, Deciding the nilpotency of the Galois group by computing elements in the centre	2043
Karim Belabas, On quadratic fields with large 3-rank	2061
Petteri Kaski and Patric R. J. Östergård, The Steiner triple systems of order 19	2075
Garikai Campbell, Points on $y = x^2$ at rational distance	2093
G. J. van der Heiden, Addendum to “Factoring polynomials over finite fields with Drinfeld modules”	2109
Reviews and Descriptions of Tables and Books	2111
Klaus Höllig 9, C. T. Kelley 10	

Editorial Information

Information on the backlog for this journal can be found on the AMS website starting from <http://www.ams.org/mcom>.

In an effort to make articles available as quickly as possible, articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

A Consent to Publish and Copyright Agreement is required before a paper will be published in this journal. After a paper is accepted for publication, the Providence office will send out a Consent to Publish and Copyright Agreement to all authors of the paper. By submitting a paper to this journal, authors certify that the results have not been submitted to nor are they under consideration for publication by another journal, conference proceedings, or similar publication.

Information for Authors

Initial submission. An author should submit the manuscript by e-mail to `mathcomp@dam.brown.edu`. The manuscript should be sent as a single postscript or pdf file. Files can be compressed using zip or gzip making the files smaller in size. If e-mail submission is not feasible, three paper copies should be submitted. If the office of the Managing Editor is not able to print the file received from an e-mail submission, the author will be contacted and asked to send three paper copies instead. The author may suggest an appropriate editor for his or her paper. All paper copies of contributions and all books for review should be addressed to Chi-Wang Shu, Managing Editor, Mathematics of Computation, Division of Applied Mathematics, Brown University, 182 George Street, Providence, RI 02912 USA. The date received, which is published with the final version of an accepted paper, is the date received in the office of the Managing Editor, and it is the responsibility of the author to submit manuscripts directly to this office.

The first page must consist of a *descriptive title*, followed by an *abstract* that summarizes the article in language suitable for workers in the general field (algebra, analysis, etc.). The *descriptive title* should be short, but informative; useless or vague phrases such as “some remarks about” or “concerning” should be avoided. The *abstract* must be brief and reasonably self-contained. Included with the footnotes to the paper should be the 2000 *Mathematics Subject Classification* representing the primary and secondary subjects of the article. The classifications are accessible from www.ams.org/msc/. The list of classifications is also available in print starting with the 1999 annual index of *Mathematical Reviews*. The Mathematics Subject Classification footnote may be followed by a list of *key words and phrases* describing the subject matter of the article and taken from it. Journal abbreviations used in bibliographies are listed in the latest *Mathematical Reviews* annual index. The series abbreviations are also accessible from www.ams.org/publications/. To help in preparing and verifying references, the AMS offers MR Lookup, a Reference Tool for Linking, at www.ams.org/mrlookup/. When the manuscript is submitted, authors should supply the editor with electronic addresses if available. These will be printed after the postal address at the end of each article.

Electronically prepared manuscripts. For the final submission of accepted papers, the AMS encourages use of electronically prepared manuscripts, with a strong preference for *AMS-L^AT_EX*. To this end, the Society has prepared *AMS-L^AT_EX* author packages for each AMS publication. Author packages include instructions for preparing electronic manuscripts, the *AMS Author Handbook*, samples, and a style file that generates the particular design specifications of that publication series. Articles properly prepared using the *AMS-L^AT_EX* style file and the \label and \ref commands automatically enable extensive intra-document linking to the bibliography and other elements of the article for searching electronically on the Web. Because linking must often be added manually to electronically prepared manuscripts in other forms of T_EX, using *AMS-L^AT_EX* also reduces the amount of technical intervention once the files are received by the AMS. This results in fewer errors in processing and saves the author proofreading time. *AMS-L^AT_EX* papers also move more efficiently through the production stream, helping to minimize publishing costs.

AMS-LATEX is the highly preferred format of *TeX*, but author packages are also available in *AMS-TeX*. Those authors who make use of these style files from the beginning of the writing process will further reduce their own efforts. Manuscripts prepared electronically in *LATEX* or plain *TeX* are normally not acceptable due to the high amount of technical time required to insure that the file will run properly through the AMS in-house production system. *LATEX* users will find that *AMS-LATEX* is the same as *LATEX* with additional commands to simplify the typesetting of mathematics, and users of plain *TeX* should have the foundation for learning *AMS-LATEX*.

Authors may retrieve an author package from the AMS website starting from www.ams.org/tex/ or via FTP to [ftp.ams.org](ftp://ftp.ams.org) (login as **anonymous**, enter username as password, and type `cd pub/author-info`). The *AMS Author Handbook* and the *Instruction Manual* are available in PDF format following the author packages link from www.ams.org/tex/. The author package can also be obtained free of charge by sending email to pub@ams.org (Internet) or from the Publication Division, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. When requesting an author package, please specify *AMS-LATEX* or *AMS-TeX*, Macintosh or IBM (3.5) format, and the publication in which your paper will appear. Please be sure to include your complete mailing address.

The final version of the electronic manuscript should be sent to the Providence office immediately after the paper has been accepted for publication. The author should also send the final version of the paper manuscript to the Managing Editor, who will forward a copy to the Providence office. Editors will require authors to send their electronically prepared manuscripts to the Providence office in a timely fashion. Electronically prepared manuscripts can be submitted via the web at www.ams.org/submit-book-journal/, sent via email to pub-submit@ams.org (Internet), or sent on diskette to the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. When sending a manuscript electronically via email or diskette, please be sure to include a message indicating in which publication the paper has been accepted. No corrections will be accepted electronically. Authors must mark their changes on their proof copies and return them to the Providence office. Complete instructions on how to send files are included in the author package.

Electronic graphics. Comprehensive instructions on preparing graphics are available starting from www.ams.org/jourhtml/authors.html. A few of the major requirements are given here.

Submit files for graphics as EPS (Encapsulated PostScript) files. This includes graphics originated via a graphics application as well as scanned photographs or other computer-generated images. If this is not possible, TIFF files are acceptable as long as they can be opened in Adobe Photoshop or Illustrator. No matter what method was used to produce the graphic, it is necessary to provide a paper copy to the AMS.

Authors using graphics packages for the creation of electronic art should also avoid the use of any lines thinner than 0.5 points in width. Many graphics packages allow the user to specify a “hairline” for a very thin line. Hairlines often look acceptable when proofed on a typical laser printer. However, when produced on a high-resolution laser imagesetter, hairlines become nearly invisible and will be lost entirely in the final printing process.

Screens should be set to values between 15% and 85%. Screens which fall outside of this range are too light or too dark to print correctly. Variations of screens within a graphic should be no less than 10%.

AMS policy on making changes to articles after posting. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue. To preserve the integrity of electronically published articles, once an article is individually posted to the AMS website but not yet in an issue, changes cannot be made in place in the paper. However, an “Added after posting” section may be added to the paper right before the References when there is a critical error in the content of the paper. The “Added after posting” section gives the author an opportunity to correct this type of critical error before the article is put into an issue for printing and before it is then reposted with the issue. The “Added after posting” section remains a permanent part of

the paper. The AMS does not keep author-related information, such as affiliation, current address, and email address, up to date after a paper is initially posted.

Once the article is assigned to an issue, even if the issue has not yet been posted to the AMS website, corrections may be made to the paper by submitting a traditional errata article to the Editor. The errata article will appear in a future print issue and will link back and forth on the web to the original article online.

Secure manuscript tracking on the Web and via email. Authors can track their manuscripts through the AMS journal production process using the personal AMS ID and Article ID printed in the upper right-hand corner of the Consent to Publish form sent to each author who publishes in AMS journals. Access to the tracking system is available from www.ams.org/mstrack/ or via email sent to mstrack-query@ams.org. To access by email, on the subject line of the message simply enter the AMS ID and Article ID. To track more than one manuscript by email, choose one of the Article IDs and enter the AMS ID and the Article ID followed by the word *all* on the subject line. An explanation of each production step is provided on the web through links from the manuscript tracking screen. Questions can be sent to mcom-query@ams.org.

T_EX files available. Beginning with the January 1992 issue of the *Bulletin* and the January 1996 issues of *Transactions*, *Proceedings*, *Mathematics of Computation*, and the *Journal of the AMS*, T_EX files can be downloaded from the AMS website, starting from www.ams.org/journals/. Authors without Web access may request their files at the address given below after the article has been published. For *Bulletin* papers published in 1987 through 1991 and for *Transactions*, *Proceedings*, *Mathematics of Computation*, and the *Journal of the AMS* papers published in 1987 through 1995, T_EX files are available upon request for authors without Web access by sending email to file-request@ams.org or by contacting the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. The request should include the title of the paper, the name(s) of the author(s), the name of the publication in which the paper has or will appear, and the volume and issue numbers if known. The T_EX file will be sent to the author making the request after the article goes to the printer. If the requestor can receive Internet email, please include the email address to which the file should be sent. Otherwise please indicate a diskette format and postal address to which a disk should be mailed. **Note:** Because T_EX production at the AMS sometimes requires extra fonts and macros that are not yet publicly available, T_EX files cannot be guaranteed to run through the author's version of T_EX without errors. The AMS regrets that it cannot provide support to eliminate such errors in the author's T_EX environment.

Inquiries. Any inquiries concerning a paper that has been accepted for publication that cannot be answered via the manuscript tracking system mentioned above should be sent to mcom-query@ams.org or directly to the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

Editorial Committee

RENÉ SCHOOF, Dipartimento di Matematica, 2a Università di Roma “Tor Vergata”, I-00133 Roma, Italy; *E-mail:* schoof@wins.uva.nl

CHI-WANG SHU, Chair. Applied Mathematics Division, Brown University, P.O. Box F, 182 George St., Providence, RI 02912-0001 USA; *E-mail:* mathcomp@dam.brown.edu

LARS B. WAHLBIN, Center for Applied Mathematics, 657 Frank H. T. Rhodes Hall, Cornell University, Ithaca, NY 14853-3801 USA; *E-mail:* awahlin@cam.cornell.edu

JOSEPH D. WARD, Department of Mathematics, Texas A&M University, College Station, TX 77843-3368 USA; *E-mail:* jward@math.tamu.edu

Board of Associate Editors

RANDOLPH E. BANK, Department of Mathematics, University of California San Diego, C-012, La Jolla, CA 92093-0001 USA; *E-mail:* reb@sdna2.ucsd.edu

CHRISTINE BERNARDI, Laboratoire d'Analyse Numerique, C.N.R.S. et Université Pierre et Marie Curie, B.C. 187, 4 place Jussieu, 75252 Paris Cedex 05, France; *E-mail:* bernardi@ann.jussieu.fr

PETER B. BORWEIN, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, BC, Canada V6T 1Z2; *E-mail:* pborwein@cecm.sfu.ca

DAVID W. BOYD, Department of Mathematics, University of British Columbia, Vancouver, BC Canada V6T 1Z2; *E-mail:* boyd@math.ubc.ca

SUSANNE C. BRENNER, Department of Mathematics, University of South Carolina, Columbia, SC 29208 USA; *E-mail:* brenner@math.sc.edu

RICHARD P. BRENT, Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, England; *E-mail:* Richard.Brent@comlab.ox.ac.uk

CARSTEN CARSTENSEN, Humboldt-Universität zu Berlin, Department of Mathematics, Unter den Linden 6, D-10099 Berlin, Germany; *E-mail:* mathcomp@math.hu-berlin.de

ARJEH M. COHEN, Faculteit Wiskunde en Informatica, TU Eindhoven, Postbus 513, 5600 MB Eindhoven, Netherlands; *E-mail:* amc@win.tue.nl

RONALD F. A. COOLS, Department of Computer Science, Katholieke Universiteit Leuven, Celestijnenlaan 200A, B-3001 Heverlee, Belgium; *E-mail:* ronald.cools@cs.kuleuven.ac.be

HOWARD ELMAN, Department of Computer Science, University of Maryland, College Park, MD 20742-0001 USA; *E-mail:* elman@cs.umd.edu

RICHARD S. FALK, Department of Mathematics, Rutgers University, Hill Center, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019 USA; *E-mail:* falk@math.rutgers.edu

DANIEL W. LOZIER, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8910, Gaithersburg, MD 20899-8910 USA; *E-mail:* dlozier@nist.gov

ZHI-QUAN LUO, Department of Electrical and Computer Engineering, McMaster University, Room CRL/225, Hamilton, ON Canada L8S 4K1; *E-mail:* luozq@mcmaster.ca

HARALD NIEDERREITER, Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore; *E-mail:* nied@math.nus.edu.sg

RICARDO H. NOCHETTO, Department of Mathematics, University of Maryland, Mathematics Building 084, College Park, MD 20742-0001 USA; *E-mail:* rhn@math.umd.edu

STANLEY OSHER, Department of Mathematics, University of California, P.O. Box 951555, Los Angeles, CA 90095-1555 USA; *E-mail:* sjo@math.ucla.edu

HAESUN PARK, Department of Computer Science, University of Minnesota, 4-192 EE/CS, 200 Union Street, Minneapolis, MN 55455 USA; *E-mail:* hpark@cs.umn.edu

JOSEPH E. PASCIAK, Department of Mathematics, Texas A&M University, 507B Blocker Hall, MS 3368, College Station, TX 77843 USA; *E-mail:* pasciak@math.tamu.edu

LOTHAR REICHEL, Department of Mathematics & Computer Science, Kent State University, P.O. Box 5190, Kent, OH 44242-0001 USA; *E-mail:* reichel@mcs.kent.edu

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, New South Wales 2109, Australia; *E-mail:* igor@comp.mq.edu.au

FRANK STENGER, School of Computing, University of Utah, Salt Lake City, UT 84112-1102 USA; *E-mail:* stenger@cs.utah.edu

DENIS TALAY, INRIA, 2004 Route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex, France; *E-mail:* talay@sophia.inria.fr

NICO M. TEMME, Centrum voor Wiskunde en Informatica, P.O. Box 94079, 1090-GB Amsterdam, Netherlands; *E-mail:* nicot@cwi.nl

HUGH C. WILLIAMS, Department of Mathematics and Statistics, University of Calgary, Calgary AB, Canada T2N 1N4; *E-mail:* williams@math.ucalgary.ca

JINCHAO XU, Department of Mathematics, Pennsylvania State University, McAllister Building, University Park, PA 16802-6401 USA; *E-mail:* xu@math.psu.edu

(Continued from back cover)

Christian Lécot and Wolfgang Wagner , A quasi-Monte Carlo scheme for Smoluchowski's coagulation equation	1953
J. Dick and F. Y. Kuo , Reducing the construction cost of the component- by-component construction of good lattice rules	1967
Ichiro Shimada , Rational double points on supersingular $K3$ surfaces	1989
Arthur Baragar , Canonical vector heights on $K3$ surfaces with Picard number three—An argument for nonexistence	2019
Neal Koblitz and Alfred J. Menezes , Obstacles to the torsion-subgroup attack on the decision Diffie-Hellman Problem	2027
Pilar Fernandez-Ferreiros and M. Angeles Gomez-Molleda , Deciding the nilpotency of the Galois group by computing elements in the centre	2043
Karim Belabas , On quadratic fields with large 3-rank	2061
Petteri Kaski and Patric R. J. Östergård , The Steiner triple systems of order 19	2075
Garikai Campbell , Points on $y = x^2$ at rational distance	2093
G. J. van der Heiden , Addendum to “Factoring polynomials over finite fields with Drinfeld modules”	2109
Reviews and Descriptions of Tables and Books	2111
Klaus Höllig 9 , C. T. Kelley 10	

MATHEMATICS OF COMPUTATION
CONTENTS

Vol. 73, No. 248

October 2004

<p>Nicolas Neuss and Christian Wieners, Criteria for the approximation property for multigrid methods in nonnested spaces</p> <p>I. Babuška and S. A. Sauter, Algebraic algorithms for the analysis of mechanical trusses</p> <p>Alan Demlow, Localized pointwise error estimates for mixed finite element methods</p> <p>Huo-Yuan Duan and Guo-Ping Liang, A locking-free Reissner-Mindlin quadrilateral element</p> <p>M. Amara, E. Chacón Vera, and D. Trujillo, Vorticity-velocity-pressure formulation for Stokes problem</p> <p>Maxim A. Olshanskii and Arnold Reusken, Grad-div stabilization for Stokes equations</p> <p>J. L. Guermond and Jie Shen, On the error estimates for the rotational pressure-correction projection methods</p> <p>James H. Bramble and Joseph E. Pasciak, A new approximation technique for div-curl systems</p> <p>Paola Pozzi, L^2-estimate for the discrete Plateau Problem</p> <p>Xavier Antoine, Christophe Besse, and Vincent Mouysset, Numerical schemes for the simulation of the two-dimensional Schrödinger equation using non-reflecting boundary conditions</p> <p>I. Alonso-Mallo, B. Cano, and J. C. Jorge, Spectral-fractional step Runge-Kutta discretizations for initial boundary value problems with time dependent boundary conditions</p> <p>Xiaobai Sun and Enrique S. Quintana-Ortí, Spectral division methods for block generalized Schur decompositions</p> <p>Marcelo Queiroz, Joaquim Júdice, and Carlos Humes, Jr., The symmetric eigenvalue complementarity problem</p> <p>Jerry Eriksson and Mårten E. Gulliksson, Local results for the Gauss-Newton method on constrained rank-deficient nonlinear least squares</p> <p>Fred J. Hickernell, Ian H. Sloan, and Grzegorz W. Wasilkowski, On tractability of weighted integration over bounded and unbounded regions in \mathbb{R}^s</p> <p>Fred J. Hickernell, Ian H. Sloan, and Grzegorz W. Wasilkowski, On strong tractability of weighted multivariate integration</p> <p>Bin Han, Thomas P.-Y. Yu, and Bruce Piper, Multivariate refinable Hermite interpolant</p>	<p style="margin-top: 150px;">1583</p> <p>1601</p> <p>1623</p> <p>1655</p> <p>1673</p> <p>1699</p> <p>1719</p> <p>1739</p> <p>1763</p> <p>1779</p> <p>1801</p> <p>1827</p> <p>1849</p> <p>1865</p> <p>1885</p> <p>1903</p> <p>1913</p>
---	--

(Continued on inside back cover)



0025-5718(200410)73:248;1-0