

# 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**

Remi Abgrall Susanne C. Brenner, Managing Editor Daniela Calvetti Zhiming Chen Ronald F. A. Cools Ricardo G. Duran Vivette Girault Nicholas I. M. Gould **Douglas Hardin** Fred J. Hickernell Gregor Kemper Boris N. Khoromskij Stig Larsson Christian Lubich Gunter Malle Michael J. Mossinghoff Stanley Osher Gilles Pagès Cheryl E. Praeger Renate Scheidler Christoph Schwab Jie Shen Zuowei Shen Igor E. Shparlinski Chi-Wang Shu Chris Smyth Daniel B. Szyld Mark van Hoeij Hans Volkmer Ya-xiang Yuan Zhimin Zhang

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718 (print) ISSN 1088-6842 (online)

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 bimonthly and is also accessible electronically from www.ams.org/journals/. Subscription prices for Volume 83 (2014) are as follows: for paper delivery, US\$669.00 list, US\$535.20 institutional member, US\$602.10 corporate member; US\$401.40 individual member; for electronic delivery, US\$589.00 list, US\$471.20 institutional member, US\$530.10 corporate member, US\$353.40 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add US\$5 for delivery within the United States; US\$35 for delivery outside the United States. Subscription renewals are subject to late fees. See www.ams.org/help-faq for more journal subscription information.

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 (ISSN 0025-5718 (print); ISSN 1088-6842 (online)) is published bimonthly 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.

© 2014 by the American Mathematical Society. All rights reserved.
This journal is indexed in Mathematical Reviews, Zentralblatt MATH, Science Citation Index<sup>®</sup>, Science Citation Index<sup>TM</sup>-Expanded, ISI Alerting Services<sup>SM</sup>, CompuMath Citation Index<sup>®</sup>, and Current Contents<sup>®</sup>/Physical, Chemical & Earth Sciences. This journal is archived in Portico and in CLOCKSS.
⊗ The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability. 10 9 8 7 6 5 4 3 2 1 19 18 17 16 15 14



## IN MEMORIAM

It is with great sadness that we report the passing away of Lars B. Wahlbin at his home in Ithaca, NY on July 13, 2013. Lars served as Managing Editor of Mathematics of Computation from 1996–2002. He served as an associate editor from 1984–1989, and editor from 1990 to 1996 and from 2002 to 2006.

Lars was born on March 25, 1945 in Linköping, Sweden. He received his Ph.D. in 1971 from Göteborg Universitet under the direction of Vidar Thomee. He was a postdoctoral fellow at the University of Chicago from 1972–1974 and in 1974 joined the faculty at Cornell University, where he spent his entire career, during which he supervised thirteen Ph.D. students.

From 2003–2012, Lars was also co-organizer of the Finite Element Circus, a regular, twice yearly conference devoted to the theory and applications of finite element methods.

Lars is most well-known for his influential work on maximum norm estimates, interior estimates and superconvergence for finite element methods. He is survived by his wife Anita, a son, daughter-in-law and two grandchildren.

# MATHEMATICS OF COMPUTATION CONTENTS

# Vol. 83, No. 285

# January 2014

Qun Lin, Hehu Xie, and Jinchao Xu, Lower bounds of the discretization	
error for piecewise polynomials	1
Johnny Guzmán and Michael Neilan, Conforming and divergence-free	1 5
Stokes elements on general triangular meshes	15
Liyong Zhu and Qiang Du, Mesh dependent stability and condition	
number estimates for finite element approximations of parabolic	97
problems	37
Bernardo Cockburn and Vincent Quenneville-Bélair, Uniform-in-time superconvergence of the HDG methods for the acoustic wave equation	65
Yanlai Chen and Bernardo Cockburn, Analysis of variable-degree HDG	05
methods for convection-diffusion equations. Part II: Semimatching	
nonconforming meshes	87
Nune Hovhannisyan, Siegfried Müller, and Roland Schäfer, Adaptive	01
multiresolution discontinuous Galerkin schemes for conservation laws .	113
Clément Cancès, Iuliu Sorin Pop, and Martin Vohralík, An a	
posteriori error estimate for vertex-centered finite volume discretizations	
of immiscible incompressible two-phase flow	153
Olivier Verdier, Reductions of operator pencils	189
Gang Bao, Shui-Nee Chow, Peijun Li, and Haomin Zhou, An inverse	
random source problem for the Helmholtz equation	215
Hatem A. Fayed and Amir F. Atiya, An evaluation of the integral of the	
product of the error function and the normal probability density with	
application to the bivariate normal integral	235
Andreas Griewank, Lutz Lehmann, Hernan Leovey, and Marat	
Zilberman, Automatic evaluations of cross-derivatives	251
Marco Streng, Computing Igusa class polynomials	275
Jan Steffen Müller, Computing canonical heights using arithmetic	
intersection theory	311
Florian Luca and Filip Najman, Errata to "On the largest prime factor	
of $x^2 - 1$ "	337
Edgar Costa and David Harvey, Faster deterministic integer factoriza-	
	339
Omran Ahmadi and Robert Granger, An efficient deterministic test for	947
Kloosterman sum zeros	347
Brendan Creutz, Second <i>p</i> -descents on elliptic curves	365
Eric Errthum, Minimal polynomials of singular moduli	411
Yannick Saouter and Herman te Riele, Improved results on the Mertens	491
conjecture Javad Doliskani and Éric Schost, Taking roots over high extensions of	421
	435
finite fields	400
prime powers	447
Eric Jespers, Ángel del Río, and Inneke Van Gelder, Writing units of	-1-1 (
integral group rings of finite abelian groups as a product of Bass units	461
module group rings of mine abenan groups as a product of Dass units	101

Wenchang Chu and Wenlong Zhang, Accelerating Dougall's ${}_{5}F_{4}$ -sum	
and infinite series involving $\pi$	475

### **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 is required before we can begin processing your paper. After a paper is accepted for publication, the Providence office will send 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. The AMS uses Centralized Manuscript Processing for initial submission. Authors should submit a PDF file using the Initial Manuscript Submission form found at www.ams.org/submission/mcom, or send one copy of the manuscript to the following address: Centralized Manuscript Processing, MATHEMATICS OF COMPUTATION, 201 Charles Street, Providence, RI 02904-2294 USA. If a paper copy is being forwarded to the AMS, indicate that it is for *Mathematics of Computation* and include the name of the corresponding author and contact information, such as an email address or mailing address. The author may suggest an appropriate editor for his or her paper.

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, reasonably self-contained, and not exceed 300 words. Included with the footnotes to the paper should be the 2010 *Mathematics Subject Classification* representing the primary and secondary subjects of the article. The classifications are accessible from www.ams.org/msc/. 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/msnhtml/serials.pdf. To help in preparing and verifying references, the AMS offers MR Lookup, a Reference Tool for Linking, at www.ams.org/mrlookup/.

Electronically prepared manuscripts. For the final submission of accepted papers, the AMS encourages use of electronically prepared manuscripts, with a strong preference for  $\mathcal{AMS}$ -EATEX. To this end, the Society has prepared  $\mathcal{AMS}$ -EATEX author packages for each AMS publication. Author packages include instructions for preparing electronic manuscripts, samples, and a style file that generates the particular design specifications of that publication series. Articles properly prepared using the  $\mathcal{AMS}$ -EATEX 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 TEX, using  $\mathcal{AMS}$ -EATEX 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.  $\mathcal{AMS}$ -EATEX papers also move more efficiently through the production stream, helping to minimize publishing costs.

 $\mathcal{A}_{\mathcal{M}}S$ -IAT<sub>E</sub>X is the highly preferred format of T<sub>E</sub>X, but author packages are also available in  $\mathcal{A}_{\mathcal{M}}S$ -T<sub>E</sub>X. 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 IAT<sub>E</sub>X or plain T<sub>E</sub>X 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. IAT<sub>E</sub>X users will find that  $\mathcal{A}_{\mathcal{M}}S$ -IAT<sub>E</sub>X is the same as IAT<sub>E</sub>X with additional commands to simplify the typesetting of mathematics, and users of plain T<sub>E</sub>X should have the foundation for learning  $\mathcal{A}_{\mathcal{M}}S$ -IAT<sub>E</sub>X. Authors may retrieve an author package for *Mathematics of Computation* from www.ams.org/mcom/mcomauthorpac.html or via FTP to ftp.ams.org (login as anonymous, enter your complete email address as password, and type cd pub/author-info). The *AMS Author Handbook* and the *Instruction Manual* are available in PDF format from the author package link. The author package can also be obtained free of charge by sending email to tech-support@ams.org or from the Publication Division, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. When requesting an author package, please specify  $A_{MS}$ -IATEX or  $A_{MS}$ -TEX and the publication in which your paper will appear. Please be sure to include your complete email address.

After acceptance. The source files for 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 submit a PDF of the final version of the paper to the Managing Editor, who will forward a copy to the Providence office. Accepted electronically prepared manuscripts can be submitted via the web at www.ams.org/submit-bookjournal/, sent via email to pub-submit@ams.org, or sent on CD to the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. When sending a manuscript electronically via email or CD, 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/authors/journals.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 computergenerated images. If this is not possible, TIFF files are acceptable as long as they can be opened in Adobe Photoshop or Illustrator.

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. 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. 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/. 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.

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**

SUSANNE C. BRENNER, Chair, Center for Computation and Technology, Johnston Hall, Louisiana State University, Baton Rouge, LA 70803 USA; *E-mail*: mathcomp@ math.lsu.edu

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

IGOR E. SHPARLINSKI, Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia; *E-mail*: igor.shparlinski@unsw.edu.au

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

### **Board of Associate Editors**

REMI ABGRALL, INRIA & Institut Polytechnique de Bordeaux, Team Bacchus and Institut de Mathematiques de Bordeaux, Bat A29 bis, 351 cours de la Liberation, 33 405 Talence, Cedex France; *E-mail*: abgrall@math.u-bordeaux.fr

DANIELA CALVETTI, Department of Mathematics, Case Western Reserve University, Yost Hall, 10900 Euclid Avenue., Cleveland, OH 44106 USA; *E-mail*: daniela.calvetti@ case.edu

ZHIMING CHEN, Institute of Computational Mathematics, Chinese Academy of Sciences, P.O. Box 2719, Beijing 100080, China; *E-mail*: zmchen@lsec.cc.ac.cn

RICARDO G. DURAN, Department of Mathematics, University of Buenos Aires, Ciudad Universitaria, Pabellon I, 1428 Buenos Aires, Argentina; *E-mail*: rduran@dm.uba.ar

VIVETTE GIRAULT, Laboratoire Jacques-Louis Lions, Boite courrier 187, Université de Pierre et Marie Curie, 4, place Jussieu, 75252 Paris Cedex 05, France; *E-mail*: girault@ann.jussieu.fr

NICHOLAS I. M. GOULD, Department of Scientific Computing, G59, R18 STFC-Rutherford Appleton Laboratory, Chilton, Oxon OX11 0QX England; *E-mail*: nick.gould @stfc.ac.uk

DOUGLAS HARDIN, Vanderbilt University Department of Mathematics 1326 Stevenson Center Nashville, TN 37240 USA; *E-mail*: doug.hardin@vanderbilt.edu

FRED J. HICKERNELL, Department of Applied Mathematics, Illinois Institute of Technology, E1 Building, Room 208, 10 W. 32nd Street, Chicago, IL 60616-3793 USA; *E-mail*: hickernell@iit.edu

GREGOR KEMPER, Technische Universität München, Zentrum Mathematik M 11, Boltzmannstr 3, 85748 Garching, Germany; *E-mail*: kemper@ma.tum.de

BORIS N. KHOROMSKIJ, Max Planck Institute for Mathematics in the Sciences, Inselstr. 22-26, D-04103 Leipzig, Germany; *E-mail*: bokh@mis.mpg.de

STIG LARSSON, Department of Mathematical Sciences, Chalmers University of Technology, SE-412 96 Gothenburg, Sweden; *E-mail*: stig@chalmers.se

CHRISTIAN LUBICH, Universität Tübingen, Mathematik, Auf der Morgenstelle 10, 72076 Tübengen; *E-mail*: lubich@na.uni-tuebingen.de

GUNTER MALLE, Fachbereich Mathematik, Universität Kaiserslautern, Postfach 3049, 67653 Kaiserslautern, Germany; *E-mail*: malle@mathematik.uni-kl.de

MICHAEL J. MOSSINGHOFF, Department of Mathematics, Davidson College, Davidson, NC 28035-6996 USA; *E-mail*: mimossinghoff@davidson.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

GILLES PAGÈS, University of Paris VI, Case courrier 188, 4, place Jussieu, 75252 Paris, Cedex 05, France; *E-mail*: gilles.pages@upmc.fr

CHERYL E. PRAEGER, School of Mathematics and Statistics, M019, University of Western Australia, 35 Stirling Highway, Crawley 6009, Western Australia, Australia; *E-mail*: praeger@maths.uwa.edu.au

RENATE SCHEIDLER, Department of Mathematics and Statistics, MS 364, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 1N4, Canada; *E-mail*: rscheidl@math.ucalgary.ca

CHRISTOPH SCHWAB, Seminar of Applied Mathematics, ETHZ, 8092 Zurich, Switzerland; *E-mail*: christoph.schwab@sam.math.ethz.ch

JIE SHEN, Department of Mathematics, Purdue University, West Lafayette, IN 47907 USA; *E-mail*: shen@math.purdue.edu

ZUOWEI SHEN, Department of Mathematics, National University of Singapore, Block S17 10, Lower Kent Ridge Road, 119076 Singapore; *E-mail*: matzuows@nus.edu.sg

CHRIS SMYTH, School of Mathematics, The University of Edinburgh, James Clerk Maxwell Building, King's Buildings, Mayfield Road, Edinburgh, EH9 3JZ, United Kingdom; *E-mail*: C.Smyth@ed.ac.uk

DANIEL B. SZYLD, Department of Mathematics, Temple University (038-16), 1805 N. Broad Street, Philadelphia, PA 19122-6094 USA; *E-mail*: szyld@temple.edu

MARK VAN HOEIJ, Department of Mathematics, Florida State University, 1017 Academic Way, Tallahassee, FL 32306 USA; *E-mail*: hoeij@math.fsu.edu

HANS VOLKMER, Department of Mathematical Sciences, University of Wisconsin-Milwaukee, P.O. Box 413, Milwaukee, WI 53201-0413 USA; *E-mail*: volkmer@csd.uwm.edu

YA-XIANG YAUN, Chinese Academy of Science, LSEC AMSS, Beijing, 100190 Peoples Republic of China; *E-mail*: yyx@lsec.cc.ac.cn

ZHIMIN ZHANG, Department of Mathematics, Wayne State University, Detroit, MI 48202 USA; *E-mail*: zzhang@math.wayne.edu

Javad Doliskani and Éric Schost, Taking roots over high extensions of	
finite fields	435
Mohammad Sadek, On elliptic curves whose conductor is a product of two	
prime powers	447
Eric Jespers, Ángel del Río, and Inneke Van Gelder, Writing units of	
integral group rings of finite abelian groups as a product of Bass units	461
Wenchang Chu and Wenlong Zhang, Accelerating Dougall's ${}_{5}F_{4}$ -sum	
and infinite series involving $\pi$	475

# MATHEMATICS OF COMPUTATION

# CONTENTS

Qun Lin, Hehu Xie, and Jinchao Xu, Lower bounds of the discretization

Vol. 83, No. 285

January 2014

	T
Johnny Guzmán and Michael Neilan, Conforming and divergence-free	
Stokes elements on general triangular meshes	15
Liyong Zhu and Qiang Du, Mesh dependent stability and condition	
number estimates for finite element approximations of parabolic	
problems	37
Bernardo Cockburn and Vincent Quenneville-Bélair, Uniform-in-time	
superconvergence of the HDG methods for the acoustic wave equation	65
Yanlai Chen and Bernardo Cockburn, Analysis of variable-degree HDG	
methods for convection-diffusion equations. Part II: Semimatching	
nonconforming meshes	87
Nune Hovhannisyan, Siegfried Müller, and Roland Schäfer, Adaptive	
multiresolution discontinuous Galerkin schemes for conservation laws .	113
Clément Cancès, Iuliu Sorin Pop, and Martin Vohralík, An a	
posteriori error estimate for vertex-centered finite volume discretizations	
of immiscible incompressible two-phase flow	153
Olivier Verdier, Reductions of operator pencils	189
Gang Bao, Shui-Nee Chow, Peijun Li, and Haomin Zhou, An inverse	
random source problem for the Helmholtz equation	215
Hatem A. Fayed and Amir F. Atiya, An evaluation of the integral of the	
product of the error function and the normal probability density with	
application to the bivariate normal integral	235
Andreas Griewank, Lutz Lehmann, Hernan Leovey, and Marat	
Zilberman, Automatic evaluations of cross-derivatives	251
Marco Streng, Computing Igusa class polynomials	275
Jan Steffen Müller, Computing canonical heights using arithmetic	
intersection theory	311
Florian Luca and Filip Najman, Errata to "On the largest prime factor	
of $x^2 - 1$ "	337
Edgar Costa and David Harvey, Faster deterministic integer factoriza-	
tion	339
Omran Ahmadi and Robert Granger, An efficient deterministic test for	
Kloosterman sum zeros	347
Brendan Creutz, Second <i>p</i> -descents on elliptic curves	365
Eric Errthum, Minimal polynomials of singular moduli	411
Yannick Saouter and Herman te Riele, Improved results on the Mertens	
conjecture	421
(Continued on inside back co	(ver)

