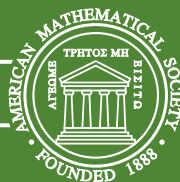


---

VOLUME 41 NUMBER 3



JULY 2004

---

# BULLETIN

( NEW SERIES )  
OF THE

---

AMERICAN MATHEMATICAL SOCIETY

---

## EDITORS

*Bulletin Articles*

Donald G. Saari  
*Chief Editor*

*Book Reviews*

Robert L. Devaney

---

PROVIDENCE, RHODE ISLAND USA

ISSN 0273-0979

*Available electronically at*  
[www.ams.org/bull/](http://www.ams.org/bull/)

## Bulletin (New Series) of the American Mathematical Society

This journal is devoted to articles of the following types:

### Bulletin Articles

Two types of articles will be included in this section: (1) papers that present a clear and insightful exposition of significant aspects of contemporary mathematical research, including Gibbs Lectures, Progress in Mathematics Lectures, and Retiring Presidential Addresses; and (2) brief, timely reports on important mathematical developments, which are normally solicited and often written by a disinterested expert.

### Book Reviews

Book Reviews are accepted for publication by invitation only. Unsolicited manuscripts will not be considered.

---

**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.** *Bulletin (New Series) of the American Mathematical Society* is published quarterly. The *Bulletin* is also accessible electronically, starting with the January 1992 issue, from [www.ams.org/journals/](http://www.ams.org/journals/). For paper delivery, subscription prices for Volume 41 (2004) are \$375 list, \$300 institutional member, \$225 individual member. The subscription price for members is included in the annual dues. A late charge of 10% of the subscription price will be imposed upon orders received from nonmembers after January 1 of the subscription year. Subscribers outside the United States and India must pay a postage surcharge of \$8; subscribers in India must pay a postage surcharge of \$15. Expedited delivery to destinations in North America is \$12; elsewhere \$28.

**Back number information.** For back issues see [www.ams.org/bookstore/](http://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 the American Mathematical Society, 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](mailto: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.)

---

*Bulletin (New Series) of the American Mathematical Society* 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, and additional mailing offices. Postmaster: Send address changes to *Bulletin*, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

© 2004 American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Science Citation Index*<sup>®</sup>, *Science Citation Index*<sup>™</sup>-Expanded, *ISI Alerting Services*<sup>SM</sup>, *CompuMath Citation Index*<sup>®</sup>, and *Current Contents*<sup>®</sup>/*Physical, Chemical & Earth Sciences*.  
Printed in the United States of America.

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

10 9 8 7 6 5 4 3 2 1 09 08 07 06 05 04

BULLETIN OF THE AMERICAN MATHEMATICAL SOCIETY  
CONTENTS

Vol. 41, No. 3

July 2004

BULLETIN ARTICLES

Jean-Pierre Bourguignon, René Thom: “Mathématicien et apprenti philosophe” .....	273
David Ruelle, Application of hyperbolic dynamics to physics: Some problems and conjectures .....	275
Steve Smale and Ding-Xuan Zhou, Shannon sampling and function reconstruction from point values .....	279
B. Mazur, Perturbations, deformations, and variations (and “near-misses”) in geometry, physics, and number theory .....	307
Michael Atiyah, The impact of Thom’s cobordism theory .....	337
Dennis Sullivan, René Thom’s work on geometric homology and bordism .....	341

BOOK REVIEWS

Juan J. Morales-Ruiz (Reviewer), Galois theory of linear differential equations, by Marius van der Put and Michael Singer .....	351
Susan Landau (Reviewer), RSA and Public-Key Cryptography, by Richard Mollin; Introduction to Cryptography, by Hans Delfs and Helmut Knebl; Cryptography: Theory and Practice, by Douglas Stinson; Algebraic Aspects of Cryptography, by Neal Koblitz; Elliptic Curves: Number Theory and Cryptography, by Lawrence Washington; Elliptic Curves in Cryptography, by Ian Blake, Gadiel Seroussi, and Nigel Smart; Modern Cryptography, Probabilistic Proofs, and Pseudorandomness, by Oded Goldreich; Foundations of Cryptography: Basic Tools, by Oded Goldreich; The Design of Rijndael: AES — the Advanced Encryption Standard, by Joan Daemen and Vincent Rijmen; Handbook of Applied Cryptography, by Alfred Menezes, Paul van Oorschot, and Scott Vanstone .....	357
J. P. C. Greenlees (Reviewer), Homotopy theoretic methods in group cohomology, by W. G. Dwyer and H.-W. Henn .....	369
Jean-Pierre Kahane (Reviewer), Trigonometric series, Vols. I, II, by Antoni Zygmund .....	377
John T. Baldwin (Reviewer), Finite structures with few types, by Gregory Cherlin and Ehud Hrushovski .....	391
Alexander Barvinok (Reviewer), Discrete convex analysis, by Kazuo Murota .....	395
Donald Sarason (Reviewer), Hankel operators and their applications, by Vladimir V. Peller .....	401

### Editorial Board for Bulletin Articles

John C. Baez  
Martin R. Bridson  
Krystyna M. Kuperberg  
Barry Mazur

Paul H. Rabinowitz  
Donald G. Saari, Chair  
Panagiotis E. Souganidis  
Michael Wolf

### Editorial Board for Book Reviews

William D. Blair  
Robert L. Devaney, Chair  
Lawrence C. Evans  
Steven Krantz

John C. Mayer  
Philip E. Protter  
Audrey A. Terras

**Chief Editor:** Donald G. Saari

### Editorial Information

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

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 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

Bulletin Articles may be of two types: (1) reasonably broad expository surveys of a currently active area of mathematical research and (2) reports on a recent accomplishment in mathematical research. 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* should be a brief technical description of the new material.

Both types of Bulletin Articles should be written so as to be understandable by graduate students or mathematicians who are not experts in the subject matter of the article. A well-written expository article will include motivating problems and examples, some indication of the historical development of the subject, and of course the results and open problems that make it an interesting and exciting area of mathematics. In most cases proofs should be at most briefly sketched, and there should be a good bibliography whose main aim is to help those wishing to pursue the subject further. Articles reporting on recent mathematical research should include an introductory section addressed to nonexperts describing the motivation, background, and significance of the results announced. Following the statement of results, there should be a sketch of proofs that may be addressed to experts, including elements of the proof which are novel. References should be given so that an interested reader can find the details.

Included with the footnotes in each 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/](http://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/](http://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/](http://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.

Bulletin Articles are normally solicited by the Editorial Board, but unsolicited manuscripts will also be considered. In particular, those giving lectures (Gibbs Lectures, Colloquium Lectures, and Progress in Mathematics Lectures) or invited hour addresses at meetings of the Society are encouraged to write up their lectures in a manner that meets the requirements for expository articles described above and to submit their manuscripts for consideration by the Editorial Board for Bulletin Articles.

For Book Reviews the first page must include the title of the book being reviewed; the name(s) of the author(s); publisher; city of publication; year of publication; number of pages, including front matter; price if known; and ISBN. There should also be a footnote with the 2000 *Mathematics Subject Classification* representing the primary and secondary subjects of the book under review. The classifications are accessible from [www.ams.org/msc/](http://www.ams.org/msc/) and are also available in print starting with the 1999 annual index of *Mathematical Reviews*. To help in preparing and verifying references, the AMS offers MR Lookup, a Reference Tool for Linking, at [www.ams.org/mrlookup/](http://www.ams.org/mrlookup/).

**Initial submission.** Bulletin Article authors may submit manuscripts for peer review as either PDF (strongly recommended) or PostScript files at <http://www.ams.org/peer-review/submission.pl>. Manuscripts must be a single file with images embedded. PostScript files will automatically be converted to PDF, and authors will have a chance to view the manuscript and data entered before releasing the manuscript into the system. Two-digit 2000 Mathematics Subject Classification numbers are included in a pull-down menu; classifications are accessible from <http://www.ams.org/msc/>. Complete author instructions are available at the site.

Authors who cannot supply PDF or PS files may submit paper copy of their manuscript to *Bulletin*/Peer-Review Submissions, 201 Charles Street, Providence, RI 02904-2294 USA. These submissions will be scanned into a PDF file and entered by AMS staff into the peer-review system. Please provide all the data required in the submission form to avoid delays in posting the manuscript.

Upon submission the manuscript will either move immediately into the AMS posting stream or go through conversion to PDF. The manuscript will then be placed in a secure area for the *Bulletin* Chief Editor, who will be notified weekly of new submissions. The Editor will collect these submissions and assign them to subject area specialists for peer review. Queries concerning the status of submissions should be sent to the Editor at [bams@math.uci.edu](mailto:bams@math.uci.edu).

**Electronically prepared manuscripts.** The AMS encourages electronically prepared manuscripts, with a strong preference for  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$ . To this end, the Society has prepared  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$  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  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$  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  $\mathcal{T}\mathcal{E}\mathcal{X}$ , using  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$  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.  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$  papers also move more efficiently through the production stream, helping to minimize publishing costs.

$\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$  is the highly preferred format of  $\mathcal{T}\mathcal{E}\mathcal{X}$ , but author packages are also available in  $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{T}\mathcal{E}\mathcal{X}$ . 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  $\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$  or plain  $\mathcal{T}\mathcal{E}\mathcal{X}$  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. L<sup>A</sup>T<sub>E</sub>X users will find that  $\mathcal{A}\mathcal{M}\mathcal{S}$ -L<sup>A</sup>T<sub>E</sub>X is the same as L<sup>A</sup>T<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  $\mathcal{A}\mathcal{M}\mathcal{S}$ -L<sup>A</sup>T<sub>E</sub>X.

Authors may retrieve an author package from the AMS website starting from [www.ams.org/tex/](http://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/](http://www.ams.org/tex/). The author package can also be obtained free of charge by sending email to [pub@ams.org](mailto: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  $\mathcal{A}\mathcal{M}\mathcal{S}$ -L<sup>A</sup>T<sub>E</sub>X or  $\mathcal{A}\mathcal{M}\mathcal{S}$ -T<sub>E</sub>X, Macintosh or IBM (3.5) format, and the publication in which your paper will appear. Please be sure to include your complete mailing address.

At the time of submission, authors should indicate if the paper has been prepared using  $\mathcal{A}\mathcal{M}\mathcal{S}$ -L<sup>A</sup>T<sub>E</sub>X or  $\mathcal{A}\mathcal{M}\mathcal{S}$ -T<sub>E</sub>X. The final version of the electronic manuscript should be sent to the Providence office immediately after the paper has been accepted for publication. Authors should also send a paper manuscript that matches the electronic manuscript to Professor Donald G. Saari, Department of Mathematics, Multipurpose Science and Technology Building, University of California, Irvine, CA 92697-3875 USA. Electronically prepared manuscripts can be submitted via the Web at [www.ams.org/submit-book-journal/](http://www.ams.org/submit-book-journal/), sent via email to [pub-submit@ams.org](mailto: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 from [www.ams.org/jourhtml/authors.html](http://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 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/](http://www.ams.org/mstrack/) or via email sent to [mstrack-query@ams.org](mailto: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 [bull-query@ams.org](mailto:bull-query@ams.org).

**T<sub>E</sub>X 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<sub>E</sub>X files can be downloaded from the AMS website, starting from [www.ams.org/journals/](http://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<sub>E</sub>X files are available upon request for authors without Web access by sending email to [file-request@ams.org](mailto: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<sub>E</sub>X 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<sub>E</sub>X production at the AMS sometimes requires extra fonts and macros that are not yet publicly available, T<sub>E</sub>X files cannot be guaranteed to run through the author's version of T<sub>E</sub>X without errors. The AMS regrets that it cannot provide support to eliminate such errors in the author's T<sub>E</sub>X 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 [bull-query@ams.org](mailto:bull-query@ams.org) or directly to the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

BULLETIN OF THE AMERICAN MATHEMATICAL SOCIETY  
CONTENTS

Vol. 41, No. 3

July 2004

BULLETIN ARTICLES

<b>Jean-Pierre Bourguignon</b> , René Thom: “Mathématicien et apprenti philosophe” .....	273
<b>David Ruelle</b> , Application of hyperbolic dynamics to physics: Some problems and conjectures .....	275
<b>Steve Smale and Ding-Xuan Zhou</b> , Shannon sampling and function reconstruction from point values .....	279
<b>B. Mazur</b> , Perturbations, deformations, and variations (and “near-misses”) in geometry, physics, and number theory .....	307
<b>Michael Atiyah</b> , The impact of Thom’s cobordism theory .....	337
<b>Dennis Sullivan</b> , René Thom’s work on geometric homology and bordism .....	341

BOOK REVIEWS

<b>Juan J. Morales-Ruiz</b> (Reviewer), Galois theory of linear differential equations by Marius van der Put and Michael Singer .....	351
<b>Susan Landau</b> (Reviewer), RSA and Public-Key Cryptography by Richard Mollin; Introduction to Cryptography by Hans Delfs and Helmut Knebl; Cryptography: Theory and Practice by Douglas Stinson; Algebraic Aspects of Cryptography by Neal Koblitz; Elliptic Curves: Number Theory and Cryptography by Lawrence Washington; Elliptic Curves in Cryptography by Ian Blake, Gadiel Seroussi, and Nigel Smart; Modern Cryptography, Probabilistic Proofs, and Pseudorandomness by Oded Goldreich; Foundations of Cryptography: Basic Tools by Oded Goldreich; The Design of Rijndael: AES — the Advanced Encryption Standard by Joan Daemen and Vincent Rijmen; Handbook of Applied Cryptography by Alfred Menezes, Paul van Oorschot, and Scott Vanstone .....	357
<b>J. P. C. Greenlees</b> (Reviewer), Homotopy theoretic methods in group cohomology by W. G. Dwyer and H.-W. Henn .....	369
<b>Jean-Pierre Kahane</b> (Reviewer), Trigonometric series, Vols. I, II by Antoni Zygmund .....	377
<b>John T. Baldwin</b> (Reviewer), Finite structures with few types by Gregory Cherlin and Ehud Hrushovski .....	391
<b>Alexander Barvinok</b> (Reviewer), Discrete convex analysis by Kazuo Murota .....	395
<b>Donald Sarason</b> (Reviewer), Hankel operators and their applications by Vladimir V. Peller .....	401



0273-0979(200407)41:3;1-C

Bulletin (New Series) of the Amer. Math. Soc.

VOLUME 41

NUMBER 3

PAGES 273–408

JULY 2004