Newsjournal of the Society for Industrial and Applied Mathematics

siam news

Volume 45/ Number 5
June 2012

Berkeley Tops Competition for Simons Institute in Theoretical CS

Richard Karp, founding director of the Simons Institute for the Theory of Computing at the University of California, Berkeley, takes an expansive view of what already seems to be a uniquely favored institute. To be situated in the heart of the Berkeley campus, with a $60 million ten-year award from the Simons Foundation, the institute was established, Karp says, to serve the worldwide community in theoretical science and to be a magnet for top scientists in the field.

Simons Institute founding director Richard Karp. Photo by Peg Skorpinski.

Early in May, shortly after learning that Berkeley had won the award, Karp gave *SIAM News* a brief tour of the landscape in which the new institute's interests lie. Many in the SIAM community, with its own varied topography, will recognize intersections and connections with their own work, and with themes of many SIAM conferences and publications.

Computational complexity, cryptography, the logic of programs, and other areas familiar to those who study the mathematical foundations of computer science will be central to activity at the Simons Institute. But by looking from a theoretical point of view at computational processes arising in a wide variety of systems—in nature, in humanly engineered edifices, on the web—the institute's leaders intend to broaden the scope of the field.

At many levels, Karp says, "nature seems to be computing in some sense." The immune system is, figuratively, executing an algorithm, he points out; protein folding can be seen as a computational process, as can evolution.

Lest he appear to be overemphasizing biology (his own recent interests include algorithmic methods in genomics), Karp cites statistical physics, with its very close ties to mathematics, as a rich area for exploration by institute scientists. Statistical physics, he points out, draws on mathematics very similar to Markov processes in such problems as finding the equilibrium configuration of a set of magnetic spins. Markov chain Monte Carlo can be used to determine the distribution of states in an Ising model in statistical physics.

See **Simons Institute** *on page 3*

Nonprofit Org
U.S. Postage
PAID
Permit No 360
Bellmawr, NJ

NAS Elects New Members

Quality trumped quantity for the SIAM community this spring when the U.S. National Academy of Sciences held its annual election of new members. Three SIAM members were among the newly elected: John Bell of Lawrence Berkeley National Lab, Wendell Fleming of Brown University, and Ruth Williams of the University of California, San Diego.

In the case of Bell and Fleming, SIAM had already recognized their contributions in one of the most meaningful possible ways: Each was the first recipient of an important new SIAM prize—the Reid Prize for Fleming (1994) and the SIAM/ACM Prize in CSE for Bell (2003, with Phil Colella). And in 2009, when SIAM inaugurated its fellows program, both were named to the initial class (Bell "for contributions to numerical methods for the partial differential equations of computational science," Fleming "for contributions to optimal control").

Fleming is currently a University Professor Emeritus in the Division of Applied Mathematics at Brown, where he spent almost his entire career. In 1994, the Reid Prize committee cited him "for pioneering research in geometric measure theory, the calculus of variations, differential games, and stochastic control and filtering."

Since his retirement in 1995, Fleming continues to live in Rhode Island, where, he says, he has been "moderately active mathematically." A sample of results from that activity include a paper on financial mathematics ("The Tradeoff Between Consumption and Investment in Incomplete Financial Markets," with Daniel Hernandez-Hernandez), and two recent papers on risk-sensitive stochastic control and differential games (all published in *Applied Mathematics & Optimization*).

John Bell, director of the Center for Computational Sciences and Engineering at LBNL, is also the deputy director of the Department of Energy's Combustion Exascale Co-Design Center. DOE established the latter to investigate numerical algorithms, data management, and programming models that will be needed to simulate combustion on exascale computer architectures.

Among the projects led by Bell at LBNL is a three-dimensional simulation of turbulent methane combustion. His work on numerical methods has included contributions in the areas of finite difference methods, numerical methods for low-Mach-number flows, adaptive mesh refinement, interface tracking, and parallel computing. In addition to combustion, he has applied these methods to problems in shock physics, seismology, flow in porous media, and astrophysics.

Ruth Williams, a Distinguished Professor in the Department of Mathematics at the University of California, San Diego, works in probability and on stochastic processes and their application. She is the current president of the Institute of Mathematical Statistics.

Also elected to NAS this year was László Lovász, a professor of computer science at Eötvös Loránd University in Budapest. He works in combinatorial optimization, algorithms, complexity, graph theory, and random walks.

REU Students Apply Wavelets to Boston's Pothole Challenge

By Dana Mackenzie

Like every city, Boston has its springtime traditions: the beginning of baseball season, the Boston Marathon . . . and potholes. In 2010, the city filled more than 7000 potholes and responded to more than 4000 complaints.

Next spring, though, there may be fewer complaints, because the smartphones of ordinary citizens will report some potholes automatically. The new pothole-detecting app, a beta version of which can be seen at http://streetbump.org, will include a wavelet-based algorithm devised by two undergraduate students and their adviser, Edward Aboufadel of Grand Valley State University in Allendale, Michigan. In February 2012, the team was one of three winners in an open "crowdsourcing" competition, organized by InnoCentive, Inc.

The pothole saga began in 2010, when the city partnered with Worcester Polytechnic professor Fabio Carrera to develop a smartphone app, called Street Bump, which collects GPS and accelerometer data from phones riding in automobiles. Unfortunately, lots of things can make a smartphone sense a bump in the road. There are speed bumps, manhole covers, and railroad tracks, and temporary obstacles like abandoned groceries; the smartphone's owner could always just drop it on the floor of the car by accident. In order to be useful, Street Bump needed an algorithm that could weed out the real potholes from the spurious incidents.

Urban blight. Potholes—thanks to a smartphone app that uses a wavelet-based algorithm devised by REU students at Grand Valley State University—could soon be less of an annoyance to city drivers (and mayors).

"It was clear that we needed some serious data analysis," says Nigel Jacob of the Mayor's Office of New Urban Mechanics. "It didn't make any sense for us to have two people in a room thinking about it. We decided it was better to task a broad audience of people."

The mayor's office turned to InnoCentive, a company based in Waltham, Massachusetts, that organizes crowdsourcing challenges. Liberty Mutual Insurance (which could presumably benefit from fewer claims on its auto insurance policies) agreed to put up $25,000 to fund the Street Bump Challenge, which began on April 28, 2011, and ran for four months.

Aboufadel had been watching the InnoCentive website for problems that his students could work on. "When I saw this, I saw something that involves detecting spikes or jumps in data," Aboufadel says. "That is something that wavelets are good for. I'm like the proverbial man with a hammer, to whom everything looks like a nail. Wavelets are my hammer."

Aboufadel posed the pothole problem to his summer research advisees, Sara Jane Parsons of Indiana University of Penn-

See **Potholes** *on page 3*

siam.
SOCIETY for INDUSTRIAL and APPLIED MATHEMATICS
3600 Market Street, 6th Floor
Philadelphia, PA 19104-2688 USA

siam news
Volume 45/ Number 5/ June 2012

U.S. Science Funding

2013 Budget Requests: A Roadmap for Federal Investments

Budgets, especially the President's budget for an upcoming fiscal year, always reflect a bit of wishful thinking. The President's budget is only the first stage in the process of allocating federal funds to programs. Both houses of Congress will have their say, and with any luck an appropriations bill will emerge some time near the October 1 beginning of the fiscal year. In a less auspicious year (often, as in the current case, an election year), an appropriation is delayed or even replaced by a continuing resolution that limits spending to some fraction of the previous year's.

Nevertheless, budgets reflect the research priorities of the agencies and the administration, and are an indication of the major themes likely to appear in the coming year's programs.

The Obama administration released its budget request for fiscal year 2013 in early March 2012. Embedded in the budget is information from the federal research-funding agencies (including the National Science Foundation, the Department of Energy's Office of Science, and the several Department of Defense agencies that fund science) about their plans for fiscal year 2013, pending appropriation of funds by Congress.

Here is what can be gleaned about the proposed budgets for some of the programs of interest to the SIAM community.

National Science Foundation

Applied mathematics and computational science are part of a number of programs across the broad spectrum of research funded by NSF. The Division of Mathematical Sciences is the home of 11 core programs, including one in applied mathematics and another in computational mathematics, as well as several important interdisciplinary programs.

Like any agency, DMS must respond to national priorities, as set by the administration, if its budget is to grow. A budget that fails to grow is able to do less over time, as the organization's buying power decreases; ultimately, the result is funding for fewer researchers and students. All the U.S. federal science agencies share some current priorities: manufacturing, innovation, cybersecurity, education, and "big data." Several agencies plan initiatives in big data: ways to handle massive sets of data and to extract useful information from them (see sidebar). National priorities have played a bigger role than usual this year in defining new research initiatives.

In 2012, despite a 2.5% increase in the overall NSF budget, DMS saw a small decrease, due in part to an NSF-wide shift of money from research to large facilities. DMS director Sastry Pantula has spoken in recent interviews of his desire to protect the core programs. Nevertheless, it is apparent from the range of new programs listed below that additional funding often comes through the creation of interdisciplinary programs.

Major Interagency Initiative on Big Data

Earlier this year the White House announced a major research initiative on challenges presented by extremely large data sets that are difficult to manage and analyze with today's techniques. NSF, in concert with other agencies, including the National Institutes of Health and the Department of Energy, has released a new solicitation, Core Techniques and Technologies for Advancing Big Data Science and Engineering.

As described in NSF's 2013 budget request, the initiative will support the development of new tools and approaches for addressing "the challenges of managing, analyzing, visualizing, and extracting useful knowledge from large, diverse, distributed, and heterogeneous data sets. This includes the development of data analytics, algorithms, and statistical and mathematical methods."

According to the interagency solicitation, "big data" refers not "just to the volume of data, but also to its variety and velocity. Big data includes large, diverse, complex, longitudinal, and/or distributed data sets generated from instruments, sensors, Internet transactions, email, video, click streams, and/or all other digital sources. The focus is on core scientific and technological advances (e.g., in computer science, mathematics, computational science and statistics)."

This program also has a major interdisciplinary component. It is, as described in the solicitation, "one component in a long-term strategy to address national big data challenges, which include advances in core techniques and technologies; big data infrastructure projects . . . and a comprehensive integrative program to support collaborations of multi-disciplinary teams and communities to make advances in the complex grand challenge science, biomedical research, and engineering problems of a computational- and data-intensive world."

Funding for CISE, NSF's Computer & Information Science & Engineering Directorate, grows by 8.5% in the 2013 budget, because computer science is perceived as essential to addressing several key priorities, including big data and cybersecurity. As Farnum Jahanian, NSF assistant director for CISE, reported to the SIAM science policy committee at its April meeting, "Think of basic research, but also how it fits into societal priorities."

Recently developed NSF programs related to priority areas include:

- Big Data Core Technologies
- CIF21 (Cyberinfrastructure Framework for 21st Century Science)
- CDS&E (Computational and Data-Enabled Science and Engineering), a joint program with the Office of Cyberinfrastructure in which DMS invested $5 million
- Secure and Trustworthy Cyberspace
- Cyber-Enabled Materials Manufacturing and Smart Systems (part of the Materials Genome Initiative).

Some of these programs have a home in CISE or OCI, with DMS as a partner. All are interesting to some segment of the SIAM community.

NSF has developed new modes of funding and new procedures for reviewing proposals, along with new programs that cut across traditional areas. New NSF-wide programs include:

■ CREATIV. A program of the Office of Integrative Activities, CREATIV (Creative Research Awards for Transformative Interdisciplinary Ventures) was established to spur innovative interdisciplinary research. Normally, proposals sent to NSF are reviewed by a panel of experts from the scientific community in the discipline(s) of the proposal; program managers make decisions based on the panel's recommendations. Under CREATIV, two program managers from separate divisions within NSF can agree to cross-fund a (good) multidisciplinary proposal. This mechanism is intended to overcome the perceived bias against multidisciplinary proposals. Awards can be made without peer review if the program managers in the separate divisions agree. According to Pantula, 75% of the funding comes from outside DMS. The program, which got a head start in 2012 with funding of $20 million, is to grow in 2013 to $60 million.

■ I-Corps. The NSF-wide Innovation Corps has been created to jumpstart a "national innovation ecosystem." Under the program, certain NSF-funded researchers will receive additional support—in the form of mentoring and funding—"to accelerate innovation that can attract subsequent third-party funding."

■ SAVI. Science Across Virtual Institutes is an example of NSF's attempt to focus on global aspects of science. Mathematics played a major role in the 2012 start-up of this program: Two NSF-funded mathematics institutes, ICERM and SAMSI, received first-round SAVI funding to create collaborative programs with institutes in India.

DOE Office of Science

The Advanced Scientific Computing Research program, known as ASCR, is the main program in the Office of Science that provides significant funding for research in applied mathematics and scientific computing.

The ASCR budget continues to emphasize multiscale/complex systems and, for 2013, adds data-intensive science. The latter is part of the national effort across several agencies to focus research on the problem of massive data, says ASCR head Dan Hitchcock. The ASCR budget proposes an allocation of $68.5 million for exascale computing, but data-intensive computing is the new piece in the ASCR program (see sidebar).

Hitchcock stresses the need for new algorithms, both compute-intensive and data-intensive, for evolving computer hardware. Because DOE is a mission agency, programs must respond to agency priorities. Accordingly, ASCR's data-intensive computing initiative focuses on kinds of data relevant to DOE, such as that coming from large facilities. And, Hitchcock notes, "The data-intensive computing initiative should be seen as part of the general push toward exascale." He points out that problems associated with data involve uncertainty quantification, and that research must also take into account the multiscale/multiphysics nature of the phenomena being investigated.

New to ASCR for 2013 will be large math centers, as described in the recent announcement of funding for Mathematical Multifaceted Integrated Capability Centers (MMICCs). In the past, ASCR's mathematics program funded about 110 projects at any time, with support mainly for individuals or small teams of five or fewer investigators.

The MMICCs program is not a small effort. As estimated in the call for pre-

See **2013 Budget** *on page 7*

siam news

ISSN 1557–9573. Copyright 2012, all rights reserved, by the Society for Industrial and Applied Mathematics, SIAM, 3600 Market Street, 6th Floor, Philadelphia, PA 19104–2688; (215) 382–9800; siam@siam.org. To be published ten times in 2012: January/February, March, April, May, June, July/August, September, October, November, and December. The material published herein is not endorsed by SIAM, nor is it intended to reflect SIAM's opinion. The editors reserve the right to select and edit all material submitted for publication.

Advertisers: For display advertising rates and information, contact Kristin O'Neill at marketing@siam.org.

One-year subscription: $64.00 U.S., Canada, and Mexico, $74.00 elsewhere. SIAM members and subscribers should allow 8 weeks for an address change to be effected. Change of address notice should include old and new addresses with zip codes. Please request address change only if it will last 6 months or more.

Printed in the USA.

siam. *is a registered trademark.*

What Lasts?

FROM THE SIAM PRESIDENT

By Nick Trefethen

At Oxbridge, the standard nickname for Oxford and Cambridge, things last a long time. There are fine old stone buildings around every corner, and my Oxford college, Balliol, was founded in 1263. I expect it will still be here in 2263. That's the Copernican Principle at work, which tells us that if you want to estimate how long something will last, a good starting guess is how long it has been here already. SIAM, for example, is pretty sure to reach 100.

So it is easy to get thinking about permanence in this environment. Indeed, England itself is one of the world's great examples of durability, having muddled along since 1066, while other nations came and went.

Who's the most famous Cambridge academic of all time? It must be Isaac Newton, and I don't think it's a coincidence that Newton was a mathematician. What he did *lasts*. And who's the most famous Oxford academic of all time? That's a trickier question. I think the best answer may be Lewis Carroll, whose real name was Charles Dodgson. Dodgson was a mathematician too, quite a good one in fact, and I don't think that's a coincidence either. What keeps *Alice in Wonderland* alive is its quirky logic, its brand of humor nearly timeless and placeless. The author of such a book had to be a mathematician.

(Admittedly, in the last few years another contender has turned up, J.R.R. Tolkien, thanks to the blockbuster *Lord of the Rings* movies. Has Tolkien, who was certainly no mathematician, grabbed the #1 spot? Well, maybe for the moment, but with a little help from Copernicus, I think Carroll will be back on top eventually.)

There is a paradox of permanence. You might think that what lasts longest should be what's strongest in the engineering sense, like stone buildings. But most of the stone around Oxford is actually more recent than, say, William of Ockham, a scholar here, or Richard the Lionheart, born here, whose names and deeds live on. Eventually material things crumble, while insubstantial things may remain. If you're a fan of the poet Shelley, who was a student here, you'll know his great poem "Ozymandias" about a stone statue decaying in the desert. I enjoy the paradox that an actual stone statue would keep decaying further, whereas the one described in Shelley's poem hasn't decayed any further at all, since it's just an idea. Shakespeare liked this kind of paradox too (but alas doesn't count as an Oxford man, though he surely passed through here on journeys to London).

Life is soft and perishable, yet outlasts rock and steel. For example, I remember being puzzled when I heard that genome studies have contributed to our understanding of how tectonic plates have moved. Comparing genes of one species and another, you can infer evidence of whether one land mass was in contact with another 100 million years ago. How can a piece of DNA be more unchanging than a continent? Of course, it's not the particular piece of DNA that lasts, but the information it carries, copied over and over again from the Cretaceous down to the present.

Charles Dodgson, aka Lewis Carroll: the most famous Oxford academic ever?

The great Oxford and Cambridge mathematician G.H. Hardy made much of the permanence of mathematics in *A Mathematician's Apology* (1940). He wrote of the enduring beauty of Euclid's proof that there are an infinite number of primes and of Pythagoras's proof that the square root of 2 is irrational:

■ "Archimedes will be remembered when Aeschylus is forgotten, because languages die and mathematical ideas do not."

■ "A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made *with ideas*."

■ "Beauty is the first test: there is no permanent place in the world for ugly mathematics."

Hardy also famously drifted into statements about applied mathematics that raise an eyebrow or two:

■ "One rather curious conclusion emerges, that pure mathematics is on the whole distinctly more useful than applied."

■ "The great modern achievements of applied mathematics have been in relativity and quantum mechanics, and these subjects are, at present at any rate, almost as 'useless' as the theory of numbers."

■ "I have never done anything 'useful'. . . . The 'real' mathematics of the 'real' mathematicians, the mathematics of Fermat and Euler and Gauss and Abel and Riemann, is almost wholly 'useless'."

■ "But is not the position of an ordinary applied mathematician in some ways a little pathetic?"

We can laugh at this stuff, but to tell the truth, Hardy's thoughts are crisp and elegant in context, and when you read the whole essay it comes across as not silly in the least. In fact it is hard not to like Hardy and enjoy his mind; but for all the permanence of his mathematics, the tone of the *Apology* seems powerfully dated, steeped in a 1930s politics now thankfully past.

Since I personally plan to last as long as possible, I hope he was wrong about this one:

■ "A mathematician may still be competent enough at sixty, but it is useless to expect him to have original ideas."

Potholes

continued from page 1

sylvania and Nathan Marculis of Grand Valley State. The two students worked on it for eight weeks as part of a Research Experiences for Undergraduates program at Grand Valley.

To begin, Parsons and Marculis used the phone's bearing and orientation information to define *x*-, *y*-, and *z*-coordinates for each incident. They weeded out incidents in which the acceleration or the velocity was too low. Then they applied a Cohen–Daubechies–Feauveau 9/7 filter (also used in JPG image compression) to enhance the detection of spikes in the acceleration data. "We used that one for a couple reasons," Aboufadel says. "It has a certain symmetry that other wavelets don't have. Also, because it averages nine data points at a time, we thought that it would be just long enough to capture the slowing down and speeding up, the typical behaviors for a pothole." The smartphone app records the acceleration three times a second, so nine data points would represent three seconds of real time.

Unfortunately, the accelerometers in a cell phone are relatively primitive, and they will often miss the moment a car hits a pothole. Other researchers—a group at MIT led by Jakob Eriksson and a group at Microsoft Research in Bangalore—equipped vehicles with accelerometers in earlier studies, but they used sophisticated instruments that could record more than 300 data points per second. Thus, a significant part of the Street Bump Challenge was to deal with low-resolution data. The teams had to collate multiple recordings by multiple vehicles along the same street, some of which recorded a bump while others didn't. Even when two cars hit the same pothole, they would not necessarily report it in exactly the same location, because of the cars' motion and because of inaccuracies in the GPS readings.

In order to detect correlated incidents, Parsons and Marculis set up a connected graph of all the reported incidents based on a road map and computed a minimal spanning tree, using Kruskal's algorithm. They then deleted the longest edges of the tree. "What's left is a forest of mini-trees," Aboufadel explains. "We assumed each cluster was an anomaly, and we computed its centroid." That gave them an estimate for the location of the pothole. "This method captured what we wanted, and it was not hard to implement. It also was easy to explain how the algorithm worked. I've done clustering with eigenvalues and eigenvectors before, and people think you're speaking Greek," Aboufadel says.

To detect correlated incidents, the students set up a connected graph of all the reported incidents based on a road map and computed a minimal spanning tree, using Kruskal's algorithm. They then deleted the longest edges of the tree.

This relatively low-tech approach worked well on the training data, identifying 9 of 11 potholes. It also worked well enough on the test data to be named one of the three prizewinners. The other two winning entrants were Elizabeth Yip, a software engineer from the state of Washington, and Sprout & Co., a community science cooperative from Somerville, Massachusetts. Each of the winning groups received a $9000 share of the prize money.

"The students are so excited," Aboufadel said. "I don't think that at the end of the summer they believed something like this could happen."

According to InnoCentive, the Boston mayor's office has already received hundreds of requests for information about the pothole-detecting algorithms. They are now combining the strong points of all three winning algorithms into one package and developing a user-friendly interface.

"There is a lot of interest out there in creating competitions to address urban challenges," says Jacob. "Our critique in general is that such challenges are incredibly broad. This was an experiment for us to see if we could take a well-articulated technical problem and get more depth in analysis. What we've seen is the development of an app that will improve the city of Boston." And maybe your city next?

Dana Mackenzie writes from Santa Cruz, California.

Simons Institute

continued from page 1

Economics comes into play, in the form of, say, auction theory. It turns out, Karp says, that algorithmic game theory can be seen in the context of computational complexity, a major theme in theoretical computer science. Here he cites a recent result by Berkeley computer scientist Christos Papadimitriou (with C. Daskalakis and P.W. Goldberg) that computing a Nash equilibrium is computationally intractable.

Consistent with Karp's descriptions is the list released in a statement by UC Berkeley of the four initial big questions to be considered at the institute: "how the diversity of life on Earth evolved in only 4 billion years"; regulatory mechanisms that govern the immune response or the genesis of cancer; database privacy; and, perhaps with the least obvious connection to theoretical computer science, improved models of climate change.

Institute scientists will not work exclusively on problems in other sciences, Karp wants to make clear. Instrinsic problems of computer science, such as P vs. NP, will be pursued, as will work in discrete analysis.

Discrete analysis, in fact, is the topic of one of the first semester-long programs the institute will run, in the fall of 2013; big data is the other. And two programs per semester will be the format for the fully operational Simons Institute, which Karp expects to draw about sixty scientists to the campus at any one time. Included in that total are four permanent faculty: Karp, as director; Alistair Sinclair, also a computer scientist at Berkeley, as associate director; and two other senior scientists with the experience and flexibility to serve as mentors as the scientific focus changes from semester to semester (filling those two positions will be a priority during the institute's first two years). Sixty scientists are expected to participate in programs each semester, including sixteen postdocs.

Among the main assets of the institute, Karp mentions interactions with other Berkeley people, groups, and centers: CITRIS, the Center for Information Technology Research in the Interest of Society, of which Jim Demmel is former chief scientist; Lawrence Berkeley National Lab; MSRI, the Mathematical Sciences Research Institute; the International Computer Science Institute (where Karp, until he took on the institute directorship, spent half of his time as head of the algorithms group); and the Miller Institute for Basic Research in Science. Not least is the university itself, which has provided both cooperation and financial support, including slots for several graduate students and, perhaps most significantly, the centrally located building, former home of chemistry labs, that is now being renovated for the institute.

Beyond, but not too far beyond, the university, lies another important resource: Silicon Valley IT firms, including Google, the institute's first founding industrial partner. In such areas as big data, search, the science of advertising, and auctions, Karp hopes that the institute will be able to draw on the expertise of the leading researchers at some of those firms. In the end, though, the Simons Institute is international. Whether through joint postdocs or participation in programs, Karp mentions connections already forged with Tsinghua University, with Microsoft India, and with others around the world. And, of course, institute leaders have ongoing ties to SIAM—"a very natural community to interact with us."—*GRC*

Mathematics as Narrative

Circles Disturbed: The Interplay of Mathematics and Narrative. *By Apostolos Doxiadis and Barry Mazur, eds., Princeton University Press, Princeton, New Jersey, 2012, 570 pages, $49.50.*

BOOK REVIEW

By Philip J. Davis

First come the symbols, then comes the narrative.

—After Bertolt Brecht

Apostolos Doxiadis, mathematician, actor, film maker, is also the author of the novel *Uncle Petros and Goldbach's Conjecture*, so it is no surprise that he is interested in mathematics and narrative. Likewise for Barry Mazur, prolific author of a large variety of popular mathematical narratives, including the 2004 *Imagining Numbers (particularly the square root of minus fifteen)*.

Circles Disturbed, a collection of 15 articles by as many authors, is so rich in content that I have found it impossible to do it justice in my allotted space. I give *Circles* a five-star rating and encourage my readers to immerse themselves in it. Though it may not be cricket, I conclude this review by pretending to be a sixteenth contributor to the book, presenting a few of my own observations on the interplay between mathematics and narrative.

Narrative-free presentations of mathematical material are easy to find. When I took second-year calculus as an undergraduate, we were advised to buy a copy of B.O. Peirce's *A Short Table of Integrals*. My edition lists 938 formulas, with hardly any narrative to expound them, to say why they're interesting or why a serious student of mathematics should pay any attention to them. I recall that Dr. John Smyth-Smith (pseud.), a brand new hot-shot TA who later became a prominent algebraic topologist, pooh-poohed Peirce's *Table*, not because it lacked narrative, but because it represented a kind of mathematics that he felt was beneath contempt.

Value judgments about mathematics are aired and enshrined in oral, written, unwritten, often unconscious, narratives that waft through our increasingly mathematized culture. They range from simple approval/disapproval to long and detailed depictions of, say, *17 Equations That Changed the World*.*

J.L. Walsh, one of my professors, said to me years later when we were writing a joint paper, "Ideally, every mathematical expression ought to be embedded in an English-language sentence." This was Walsh's beau ideal of mathematical expository style. I've kept his admonition in mind over the years, hoping to adhere to it. But looking over some of the mathematical material I've produced, I find that I pretty much abandoned it.

Take a look at the chapter on the gamma function that I wrote for the famous Abramowitz and Stegun *Handbook of Mathematical Functions*. It introduces the gamma function by Euler's integral, and it's full of isolated identities, such as $\Gamma(1 + iy) = iy\, \Gamma(iy)$. But there are no accompanying narratives.

Timothy Gowers, one of the *Circles* authors, illustrates that while the same mathematical fact or theory can be introduced in a variety of ways, some presentations will be distinguished for their vividness. It's not easy to recover what was in my mind more than a half century ago, but having produced my chapter in Abramowitz and Stegun, I must have felt a crying need for an embedding narrative that would produce vividness, for I went on to write *A Historical Profile of the Gamma Function* (*The American Mathematical Monthly*, December 1959).

*Ian Stewart, *In Pursuit of the Unknown: 17 Equations That Changed the World*, Basic Books, 2012.

Thus, I agree heartily with David Corfield's suggestion, in the chapter "Narrative and the Rationality of Mathematical Practice," that though mathematics is traditionally considered the logical discipline par excellence, to be fully rational, mathematicians must embrace narrative as a basic tool for understanding the nature of their discipline and research.

Mazur presents and discusses a possible taxonomy of narratives: (1) origin stories, (2) purpose stories, (3) "raisins in the pudding," (i.e., the purely ornamental), and (4) dreams, their consequences and motivations. Interested mainly in (4), Mazur considers what it means for a mathematician to have a dream: "Kronecker's dream is to provide us with some way of explicitly understanding *fields* of *algebraic numbers* that are *abelian* over a given *number field*." I suppose that narratives of all these types can be found in current expository mathematical material.

Consider mathematical narratives that attempt to interpret very old texts. Methodologies of interpretation go by the fancy name "hermeneutics," and a frequently utilized interpretive device goes by the name "present-centered history." The interpreter in the latter describes the past using full knowledge of developments of subsequent importance. But can the interpreter do better than that and really get into the minds of the past creators? Only imperfectly. Eleanor Robson, known for studies of ancient Babylonian mathematics, has suggested as much. Nonetheless, efforts have been made in this direction; Robson referred† to the work of Henk Bos and Herbert Mehrtens, who considered the relation between mathematics and the enveloping society, and of David Bloor, for whom mathematics was a social construction tout court.

The creation of new mathematics is often said (perhaps fallaciously) to be limited to the young. The later careers of research mathematicians read like a salad bar of biographical possibilities. In my own case, having produced *N* technical papers in the manner accepted by the research establishment, but not wanting to abandon the subject that has yielded me much bread, butter, and pleasure, I switched over to mathematical history, philosophy, metaphysics, pragmatics, and even journalism and interviews. In these areas narrative reigns supreme. What follows is an instance of this sort of narrative.

■■■

On the basis of the following characteristics, I see the Unity of Mathematics as a dream, a chimera, an ideal.

■ The subject classification scheme. To some extent, each of the close to a hundred mathematical areas has its own techniques, intellectual resources, and devotees, although there may be tenuous connections between, say, potential theory and non-associative algebras, and rare collaborations between experts that indicate a certain degree of unity and coherence in the field of mathematics. I find the lack of unity more strikingly located elsewhere.

■ Diachronic and cross-cultural disunity. Written mathematics is easily 4000 years old. It has been created by people and has served a variety of purposes for them. A mathematician lives in a sub-culture at a certain time and place. A piece of mathematics does not exist only as a sequence of special symbols, because the naked symbols are essentially uninterpretable. The symbols are embedded in a cloud of knowledge, meanings, associations, experiences, imaginations that derive from the particularities of time, place, person, and the enveloping society.

Pythagoras asserted that 3 is the first male number. In certain Christian theologies, 3 is the number of the Godhead. If, in Indian numerology, the numbers 1,10,19, and 28 are "ruled by the sun," the meaning of and the belief in those words may, as Eleanor Robson would suggest, escape my readers.

†*Mathematics in Ancient Iraq: A Social History*, Princeton University Press, 2008.

The universality of mathematical narrative. Atsuko Tanaka (1932–2005), in her 16mm film Round on Sand *(Japan, 1968). Copyright 2010 Ryoji Ito and Takehiro Nabekura, courtesy of the Ashiya City Museum of Art & History. Photo by Takehiro Nabekura.*

■ Semantic ambiguity. I could write down the sequence of symbols x╚∩σΣ ≡ 6 and claim that it is a piece of mathematics. But this claim could not be substantiated solely on the basis of the symbols. To provide meaning, every mathematical statement must be embedded in a narrative in some natural language (English, German, et alii). Furthermore, its significance as mathematics cannot be established if knowledge of it is limited to one person as a private revelation.

■ Semiotic ambiguity. Can it be determined when two mathematical statements, phrased differently, assert the same thing? Barry Mazur begins a discussion of this question in the book under review in a chapter titled "Visions, Dreams, and Mathematics."

■ Non-acceptance or doubts about certain theories put forth by professional mathematicians. Examples are easily found. Originally, there was one formal geometry: that of Euclid. After Bolyai and Lobatchevski, there were three, and since Riemann, we have had an infinity of geometries.

Zermelo did not believe Gödel's proof. For George Berkeley, infinitesimals were the "ghosts of departed quantities." Skepticism regarding the concepts of Cantor has been expressed by many, including Kronecker, Poincaré, Zermelo, E. Picard, Brouwer, Hermann Weyl, Wittgenstein, Errett Bishop.

A well-known quote from the great applied mathematician Richard Hamming sums this up:

"I know that the great Hilbert said 'We shall not be driven out of the paradise that Cantor has created for us,' and 'I reply I see no reason for walking in.' "

■ Philosophic ambiguity. Prior to the end of the 19th century, there was one philosophy of mathematics: platonism. Now there are easily five distinguishable philosophies, together with variations that exhibit the Freudian "narcissism of slight differences."

And yet. . . . There is a unique corpus of material, a creation of human intellect that is called mathematics, in which narrative plays a vital role. But tell me, in what does the often touted unity of mathematics consist?

Acknowledgments

I thank Bernhelm Booss-Bavnbeck for numerous discussions about the themes considered in this review.

Philip J. Davis, professor emeritus of applied mathematics at Brown University, is an independent writer, scholar, and lecturer. He lives in Providence, Rhode Island, and can be reached at philip_davis@brown.edu.

Probing the Deep Mathematics of Nonlinear Inverse Problems

As the SIAM News *liaison for the SIAM Activity Group on Imaging Science, Samuli Siltanen suggested that readers might be interested in the work of the most recent recipient of the Calderón Prize, Guillaume Bal. The prize, given biannually by the Inverse Problems International Association, recognizes researchers under the age of 40 who have made significant advances in the mathematics of inverse problems; it was awarded to Bal at the 2011 Applied Inverse Problems Conference at Texas A&M University.*

Inverse problems are about deciphering indirectly measured data of an unknown quantity, such as the inner structure of a patient. The aim is to go from an effect to the cause, as opposed to the simpler direct problem of going from cause to effect. In medical X-ray tomography, for example, the direct problem is to determine what kind of X-ray images (effect) we would get from different directions when imaging a patient whose inner structure (cause) we know. The inverse problem is the more difficult task of producing a three-dimensional reconstruction of the patient based on several two-dimensional X-ray images.

X-ray tomography is a linear inverse problem. For many medical measurements, by contrast, the body is probed with energy whose propagation depends on the medium, leading to nonlinear inverse problems. An example is electrical impedance tomography, which is based on feeding harmless electric currents into the body and reconstructing the inner conductivity distribution from the resulting voltages at the skin. The boundary measurements depend on the conductivity in a nonlinear way. Another example is the classic diagnostic method of manual palpation, which can be viewed as boundary measurements based on elastic deformations. Quite deep and interesting mathematics has been needed, and created, for the analysis of nonlinear inverse problems.

In recent years, Guillaume Bal has made a variety of mathematical contributions to the study of nonlinear inverse problems, concentrating for the most part on cases in which the propagation of the probing energy is modeled by partial differential equations. His studies cover a broad scientific domain, including integral geometry, direct and inverse transport models, Monte Carlo methods, asymptotic models for equations with random coefficients, and time-reversal imaging in random media. He has a special interest in hybrid inverse problems arising from coupled-physics measurements.

The solution of hybrid inverse problems is typically done in two steps. In the first, one solves an inverse boundary-value problem that provides high-resolution information about an internal structure. The internal functional revealed in this way can be viewed as another indirect measurement. The second step consists of solving the

See **Inverse Problems** *on page 6*

Elliptic Curve Groups and Their Cryptographic Applications

Elliptic Tales: Curves, Counting, and Number Theory. *By Avner Ash and Robert Gross, Princeton University Press, Princeton, New Jersey, 2012, xxii+253 pages, $29.95.*

BOOK REVIEW
By James Case

The Birch and Swinnerton-Dyer conjecture is perhaps the least well-known of the Clay Institute's seven million-dollar challenge problems. It concerns "rational points"—points whose Cartesian coordinates x and y are both rational numbers—on elliptic curves. With the development of "elliptic curve cryptography" in the last quarter century, such curves have been increasingly important for modern communication systems. Neal Koblitz and Victor S. Miller suggested the application in 1985, when they independently observed that the protocols employed since the mid-1970s in public-key cryptography could be modified to work in arbitrary finite groups, including elliptic curve groups.

Second-generation Public-key Cryptography

First-generation public-key systems, such as RSA and Diffie–Hellman, make use of the multiplicative group of non-zero elements of F_p, the field of residues modulo a large prime number p. Second-generation systems, utilizing elliptic curve groups, offer a variety of advantages: more security per bit of key size than either RSA or DH, lower transmission costs, and more efficient use of electrical power. The degree of security attained with an RSA or DH key of 3072 bits, for instance, is no greater than that for an elliptic curve key of only 256 bits, at a fraction of the monetary cost and electric power consumption. Moreover, the advantages of elliptic curves only increase with enhanced security levels. Power consumption is particularly important for financial transactions, now so routinely conducted with the aid of smartcards and low-power smartcard readers.

The majority of public-key systems in use today employ 1024-bit keys for RSA and DH authentication protocols. In 2005, the National Institute of Standards and Technology declared that such protocols would be adequate through 2010, but recommended their replacement thereafter by more secure alternatives. Since 2005, NIST has published and updated a list of as many as 15 elliptic curves of varying sizes that it deems suitable for current cryptographic use. The National Security Agency is gradually transitioning to elliptic curve-based public-key systems for protecting both classified and unclassified information, as are both the U.S. Department of Defense and NATO.

Various firms and individuals have been granted patents for proprietary implementations of elliptic curve cryptography. The Canadian company Certicom holds more than 130 such patents, and NSA recently purchased a license covering 26 of them as they apply to agency activities. The firm intends to market software toolkits to NSA licensees, and perhaps to others as well.

Theory of Rational Cubic Curves

The theory of rational points on "rational cubic curves," of which elliptic curves are a special case, has been under development since the 19th century. Because there is no known method for deciding in a finite number of steps whether a rational cubic curve contains a rational point, the existing theory is confined to curves known in advance to contain at least one such point,* hereinafter denoted ∞. The corresponding problem for rational quadratics has a complete (if not quite elementary) solution, while that for rational curves of higher order seems to be intractable.

The equation of any rational cubic curve possessing at least one rational solution can be reduced, via well-known transformations, to its Weierstrass *normal form*

$$y^2 = x^3 + Ax + B. \qquad (E)$$

It is occasionally important to distinguish between the equation (E) and the "curve" C consisting, for some field K, of elements (x,y) of $K \times K$ that satisfy (E). Common choices of K are $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and the field F_p mentioned above. Whereas the question of rational points on curves C satisfying (E) makes sense for rational coefficients A and B, the bulk of the existing theory pertains to the case in which both are integers. The possible shapes of such curves are quite diverse, as shown in Figure 1.

The reason it is possible to construct an elaborate theory of rational points on elliptic curves is that such points form finitely generated abelian groups. Although usages differ, most writers call the curve C associated with a particular equation (E) "elliptic" only if all three roots of $x^3 + Ax + B$ are distinct, forcing elliptic curves to have unique tangents at every point on the curve. A complete theory, however, requires consideration, as discussed below, of "singular cubics" for which two or more of the roots coincide. The null set of a polynomial $f(x,y)$ can fail to have a unique tangent only at singular points (x,y) at which $f_x = f_y = 0$.

If an elliptic curve C contains two rational points P and Q, it must contain a third—perhaps at infinity—denoted $P * Q = Q * P$. Addition on C can then be defined as $P + Q = \infty * (P * Q)$. Under that operation, the rational points on an elliptic curve C known to contain a rational point ∞ can be shown to form an abelian group G^+, with ∞ as identity element. The English mathematician Louis Mordell showed in 1922 that G^+ is finitely generated.

Given a rational point P on an elliptic curve C, one can form P, $2P = P + P$, $3P = P + P + P$, etc. If any two points in the resulting sequence are equal, say $jP = kP$, then $mP = (k - j)P = \infty$, and P is said to be of "finite order" m. Some but not all elements of G^+ will ordinarily be of finite order, so that the entire group is generated by $P_1, \ldots, P_t, P_{t+1}, \ldots P_{t+r}$, where t is the number of generators of finite order, and r the number of generators of infinite order, known as the "rank" of G^+. A theorem discovered independently by Trygve Nagell (1935) and Elizabeth Lutz (1937) demonstrates that the rational points of finite order are in fact integer points, and makes it possible to calculate their generators from the prime factors of the discriminant $\Delta_E = -16(4A^3 + 27B^2)$ of (E).

*A curve is called rational and cubic if it is the null set of a cubic polynomial in two variables with rational coefficients.

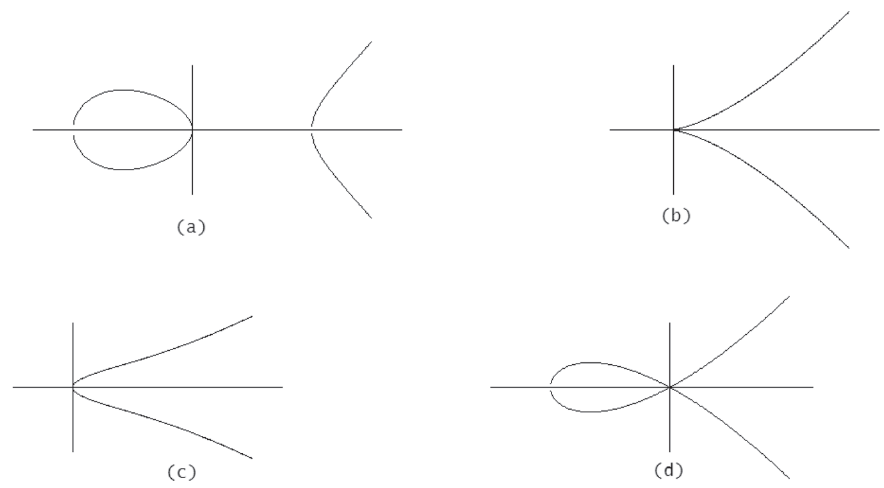

Figure 1. *Solution sets of (E) can assume a variety of shapes. The forms in (a) and (c) are deemed elliptic, those in (b) and (d) are not, due to the singularity (lack of a unique tangent) at the origin of coordinates.*

Some forty years later, motivated by the fact that 19th-century mathematicians had identified elliptic curves containing rational points of order 2,3,4,5,6,7,8,9,10, and 12, but had never found any containing points of order 11, 13, or higher, Barry Mazur proved a far more intricate theorem: t is either 1 or 2, and the subgroup of G^+ consisting of elements of finite order—traditionally known as the "torsion subgroup" of G^+—is cyclic, of order 2,3,4,5,6,7,8,9,10, or 12, unless it is the direct product of a cyclic subgroup of order 2,4,6, or 8 and another of order 2. In consequence, the torsion subgroup of G^+ cannot contain more than 16 elements, and no longer seems particularly mysterious. It is much harder to say anything of consequence about the subgroup consisting of elements of infinite order. To date, the cryptographic applications involve only the finite elliptic curve groups, for which $r = 0$, but who knows what the future may hold?

From the Weak to the Strong Form of B&SD

The original (weak) form of the Birch and Swinnerton-Dyer conjecture identifies a possible shortcut to the determination of r, while the more recent strong form suggests a way in which the r generators of infinite order can actually be calculated. The technique begins with a remarkable generalization of Euler's famous identity

$$\Pi_p\,(1 - 1/p^s) = \zeta(s) = \Sigma_n\, 1/n^s,$$

in which the product extends over all primes p and the sum over all integers $n > 0$. The required generalization is

$$\Pi_{p \in S} 1/(1 - a_p p^{-s}) \cdot \Pi_{p \in S'}\, 1/(1 - a_p p^{-s} + p^{1-2s}) = L(E,s) = \Sigma_n\, a_n/n^s,$$

where the sum extends over all integers $n > 0$, while the sets S and S' over which the two products extend consist, respectively, of primes p that do and do not divide the discriminant Δ_E. The distinction is important because $E(\mathrm{mod}\ p)$ becomes singular when p divides Δ_E.

Because the coefficients a_n appearing on both sides of the identity depend multiplicatively on the index n, in the sense that $a_{mn} = a_m \cdot a_n$, it suffices to know the values a_p for primes p. If $p \in S'$, then $a_p = p + 1 - N_p$, where N_p is the number of elements of $F_p \times F_p$ that satisfy $E(\mathrm{mod}\ p)$, the restriction of (E) to F_p. If $p \in S$, a_p is either 0, 1, or –1, according to which of three mutually exclusive conditions prevails.

The function $L(E,s)$ so constructed is called the L-function associated with (E). Because its Dirichlet series expansion can be shown to converge absolutely in the right half $Re(s) > 3/2$ of the complex s-plane, $L(E,s)$ is analytic there and can be continued analytically—just like the Riemann zeta function—to the entire complex s-plane. Also like the Riemann zeta function, the function $\Lambda(E,s)$ derived from $L(E,s)$ by the formula $\Lambda(E,s) = (\sqrt{N}/2\pi)^s\Gamma(s)L(E,s)$ can be shown to satisfy the handy functional equation $\Lambda(E,s) = w\Lambda(E, 2 - s)$, in which w is either 1 or –1.

Being analytic in the entire complex s-plane, $L(E,s)$ has a Taylor series expansion $c(s - 1)^\rho + d(s - 1)^{\rho+1} + \ldots$ about $s = 1$. The original (weak) form of the Birch and Swinnerton-Dyer conjecture asserts only that $\rho = r$, the rank of G^+, while the more recent strong form proposes a rather complicated algorithm for evaluating first the leading coefficient c and then the r infinite-order generators of G^+. In the final chapter of their book, Ash and Gross point out that the conjecture has been confirmed for $r = 0$ and $r = 1$, and go on to describe some of the computer-aided experiments that led Birch and Swinnerton-Dyer, around 1960, to formulate their conjecture. Those who remember what machine computation was like in the late 1950s will find that part of the story particularly impressive.

If there were nothing more to the story, Ash and Gross would have had no need to write a book. Their stated purpose is to explain the matter in a fashion understandable to a "mathematically inclined high school graduate." To that end, they devote the whole of Part I to explaining the conventions regarding multiple and complex roots of polynomials, homogeneous coordinates, and "points at infinity" needed to justify the conclusion that every cubic curve meets every straight line in exactly three points. Part II explores the anatomy of the group G^+ associated with an arbitrary cubic curve C, be it singular or nonsingular, before delving in Part III into enough complex function theory to make sense of $\zeta(s)$, $L(E,s)$, and $\Lambda(E,s)$, together with their power and Dirichlet series expansions, analytic continuations, and the functional equations they satisfy.

It would take an unusually ambitious high school student to get through the whole of the book in a single summer. Yet a student who received it as a graduation present, and returned to it in subsequent summers, could well have a rewarding experience.

One cannot help being impressed, in reading the book and pursuing a few of the references, by the magnitude of the enterprise it chronicles. From the 19th-century discovery of rational points of orders 2–10 and 12 on elliptic curves, to the 20th-century revelation of the structure of G^+, to the ongoing efforts to resolve the B&SD conjecture, the number, stature, and dedication of those involved are indeed awesome.

James Case writes from Baltimore, Maryland.

Inverse Problems

continued from page 4

inverse problem of interpreting the latter data. The advantage of this procedure is that the second step would be extremely sensitive to measurement errors if the data were collected at the boundary; the virtually collected inner data allows a more stable solution and leads to better resolution.

Photo-acoustic tomography, or PAT, is a prime example of a hybrid inverse problem. In the first step, infrared light pulses are sent into tissue, leading to local thermal expansion at the sites of energy absorption. This rapid expansion creates ultrasound waves that can be detected when they arrive at the skin, allowing a high-resolution reconstruction of the distribution of optical energy absorption. In the second step, optical properties of the tissue are recovered from the internal information provided by the first step. Combining the high resolution of acoustic waves with the large contrast of optical waves, PAT is sometimes called the lightning-and-thunder method. Bal's recent work has greatly advanced the understanding of the fundamental properties and possibilities of PAT.

■ ■ ■

In the inverse problems research community, Bal is known as an energetic mathematician whose enthusiasm is catching. In September 2011, during a conference in Edinburgh, I had the chance to interview him for *SIAM News*.

Among mathematical disciplines, what is it about inverse problems in particular that drew you into the field?

It all started when Oliver Dorn and I met as postdocs at Stanford and discussed the mathematics of inverse problems. Also, an important role was played by the MSRI theme year on inverse problems in 2001. I was working with a time-reversal problem related to transport equations, and the talks at a workshop in November 2001 revealed a variety of new and fascinating mathematical questions.

The main reason for my continuing interest is the fruitful interaction between applications and theory, which is a characteristic feature of inverse problems.

What is the role of hybrid, or combined, imaging modalities among traditional methods?

From the practical point of view, it is advantageous to combine two measurements, one having high contrast, the other high resolution. There are a bunch of candidates for practically useful hybrid imaging methods. Judging their potential is based on analyzing the strength of the physical interactions involved: Is there enough signal to yield information?

From the theoretical point of view, hybrid inverse problems lead to the study of so-called internal functionals. There are lots of open problems and new fundamental questions about them, so there is no lack of exciting research work to be done. On one hand, new tools are needed for analyzing these internal functionals, and on the other hand, some old tools are readily applicable. So both challenges and ways to proceed are available.

Warming to the topic, Bal continues his comments on hybrid inverse problems.

The connection to the theory of nonlinear PDEs is interesting as well—traditionally, nonlinear inverse problems arise from linear PDE models, but in hybrid cases the models are often nonlinear.

A long-term research objective is to provide a comprehensive classification of inverse problems with internal functionals.

Which one of your published results are you the most proud of?

It's really hard to pick out just one paper. I mean, could you pick one of yours? If I have to, it would be the article "Ray Transforms in Hyperbolic Geometry," concerning nonlinear tomography in hyperbolic geometry, with applications to single-photon emission computed tomography (SPECT). There the tomographic reconstruction task is reduced to a Riemann–Hilbert problem.

For Guillaume Bal, hybrid inverse problems, which often arise from nonlinear PDE models, are one of the most exciting areas of his recent work.

Rather than promote a single paper, though, I would say that the recent activity on hybrid inverse problems is the most exciting cohesive work I've done in the field of inverse problems theory.

How do you see the future of inverse problems?

Well, new measurement techniques do create new questions all the time, and the theory of inverse problems provides tools for answering them. There will surely be a continuous feed of interesting problems offered by future technologies.

■ ■ ■

Guillaume Bal received a PhD at the University of Paris VI in 1997 under the supervision of Yvon Maday. For his PhD thesis, "Coupling of Equations and Homogenization in Neutron Transport," he received the Jean-Pierre Lepetit Prize for the best PhD thesis defended in 1997–1998 at the Direction des Études et Recherches d'Electricité de France (EDF). He is currently a professor of applied mathematics at Columbia University.

Previous winners of the Calderón Prize were Matti Lassas (2007) and Martin Burger (2009). Lassas is known as a versatile mathematician who has provided innovative solutions to analytic and geometric inverse problems, to questions of invisibility, and to practical imaging problems, such as three-dimensional dental X-ray tomography. Martin Burger, a similarly multi-faceted mathematician, has created and analyzed reconstruction algorithms for medical imaging and image processing. He is an expert on the theory and application of sparsity-promoting inversion, such as total variation regularization and level set methods.—*Samuli Siltanen, University of Helsinki.*

Medicare Auctions

continued from page 8

What he has learned so far suggests that the market structure was "turned upside-down" by the auctions. "The existing providers were largely thrown out and replaced by people who haven't provided before," he says.

If CMS continues to expand its auctions, Cramton predicts that the companies that will survive are the ones willing to accept the low prices and compromise on quality. "I think there's going to be a real race to the bottom."

Cramton is working with members of Congress toward a requirement that CMS make its auctions similar to the spectrum auctions. Meanwhile, he says, there's a moral to the story: "No one would build a bridge without consulting a bridge expert. If you want to design an auction, you have to consult an auction expert. Any expert could have told CMS there were problems with what they were trying to do."

Erica Klarreich writes from Berkeley, California.

Professional Opportunities

Send copy for classified advertisements to: Advertising Coordinator, SIAM News, *3600 Market Street, 6th Floor, Philadelphia, PA 19104–2688; (215) 382–9800; fax: (215) 386–7999; marketing@siam.org. The rate is $2.55 per word (minimum $295.00). Display advertising rates are available on request.*

Advertising copy must be received at least four weeks before publication (e.g., the deadline for the September 2012 issue is July 31, 2012).

Advertisements with application deadlines falling within the month of publication will not be accepted (e.g., an advertisement published in the September issue must show an application deadline of October 1 or later).

Students (and others) in search of information about careers in the mathematical sciences can click on "Careers and Jobs" at the SIAM website (www.siam.org) or proceed directly to

www.siam.org/careers

Institute for Computational Engineering and Sciences

Institute for Computational Engineering and Sciences

ICES

The *Institute for Computational Engineering and Sciences (ICES)* at *The University of Texas at Austin* is engaged in a comprehensive initiative to bring advances in computer modeling and simulation to bear on the scientific and engineering Grand Challenges that affect our nation's well-being and competitiveness. In support of this goal, the ICES Initiative for Simulation-Based Engineering and Sciences is searching for outstanding researchers in computational science and engineering to fill endowed faculty positions at the Associate Professor level and higher. Searches are under way to find world leading researchers in three areas: 1) computational geophysical fluid dynamics, with particular interest in ocean modeling; 2) structural bioinformatics, the computational modeling of structure and function of biological macromolecules; and 3) the broad area of predictive science and uncertainty quantification in computational science and engineering. These endowed positions will provide the successful candidates with the resources and environment needed to tackle frontier problems in science and engineering via advanced modeling and simulation. The initiative builds on the world-leading program at ICES in Computational Science, Engineering and Mathematics (CSEM), which features 16 research centers and groups as well as a graduate degree program in CSEM.

Candidates for these new positions are expected to have an exceptional track record in interdisciplinary research at the intersection of advanced mathematical and computational techniques and target scientific and engineering problem. To be considered, please visit: *www.ices.utexas.edu/moncrief-endowed-positions-app/.*

The University of Texas at Austin is an Affirmative Action/Equal Employment Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, disability, age, citizenship status, Vietnam era or special disabled veteran's status, or sexual orientation. This is a security sensitive position; background check on selected applicant is required.

The University of Texas at Austin

Utrecht University, Netherlands

Mathematical Institute

The Mathematical Institute at Utrecht University invites applications for two full professorships in mathematics (0.8–1.0 fte). It is anticipated that one appointment will be made in the section of fundamental mathematics, currently comprising algebra, analysis and geometry, and one in the section of mathematical modelling, currently comprising applied analysis, stochastics, and mathematics of computation; however, the search is not limited to these areas and, in the case of exceptional candidates, both appointments could be made in the same section. The institute is looking for outstanding candidates who will invigorate and enrich the pool of expertise in the institute and the university at large. Appointees are expected to play an active role in all aspects of academic life. Candidates should demonstrate excellence in research, including grant-earning capacity, and be skilled in teaching and student supervision. The institute also expects a willingness to take up administrative responsibilities. The appointments are, in principle, permanent, at the level of full professor on a "Core Chair"; however, the institute may offer more junior candidates of exceptional promise a "Profile Chair," which is subject to review after a five-year period.

The Mathematical Institute has a long-standing tradition of crossing borders into other scientific fields. Interdisciplinary activities include, but are not limited to, theoretical physics, theoretical biology, and life sciences.

Applicants should see http://www.math.uu.nl/jobs for a complete job description and http://www.math.uu.nl/facts.html for a fact sheet concerning the institute. The closing date for applications is August 1, 2012.

Utrecht University specifically encourages female candidates to apply.

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Professor of Applied Mathematics

The Department of Mathematics (www.math.ethz.ch) at ETH Zurich invites applications for a position in Applied Mathematics at the Full or Associate Professor level. The vacant position is within the Seminar for Applied Mathematics, SAM (www.sam.math.ethz.ch).

The successful candidate's mathematical results should have received wide international recognition. His or her results should be landmark contributions to mathematical modelling and/or efficient numerical simulation in engineering and the sciences. A strong algorithmic and computational component in his/her mathematical research is expected. The candidate should have demonstrated proficiency in conducting pioneering projects in applied mathematics. Together with other members of the Department, the new professor will be responsible for teaching undergraduate courses (German or English) and graduate courses (English) for students in Applied Mathematics and Computational Science and Engineering (CSE).

Please apply online at **www.facultyaffairs.ethz.ch**. Your application should include your curriculum vitae and a list of publications. The letter of application should be addressed **to the President of ETH Zurich, Prof. Dr. Ralph Eichler. The closing date for applications is 31 July 2012**. ETH Zurich is an equal opportunity and affirmative action employer. In order to increase the number of women in leading academic positions, we specifically encourage women to apply. ETH Zurich is further responsive to the needs of dual career couples and qualifies as a family friendly employer.

Announcements

Send copy for announcements to: Advertising Coordinator, SIAM News, *3600 Market Street, 6th Floor, Philadelphia, PA 19104–2688; (215) 382–9800; marketing@siam.org. The rate is $1.65 per word (minimum $225.00). Announcements must be received at least one month before publication (e.g., the deadline for the September 2012 issue is July 31, 2012).*

University of South Carolina

Call for Nominations: 2013 Vasil Popov Prize

Nominations are being accepted for the 2013 Vasil Popov Prize. The prize is awarded every three years for outstanding research in fields related to the work of Vasil A. Popov, who is best known for his contributions to approximation theory. Candidates must have received a PhD within the previous six years.

Nominations, which should include a brief description of relevant work and a vita of the nominee, should be sent to: Pencho Petrushev, Chair, Popov Prize Selection Committee, Interdisciplinary Mathematics Institute, University of South Carolina, Columbia, SC 29208; popov.prize@gmail.com. The deadline for nominations is November 15, 2012. The prize will be awarded in April 2013 at the 14th International Conference in Approximation Theory, in San Antonio, Texas.

For further information, readers can visit http://imi.cas.sc.edu/popov-prize-call-nominations/.

Solar Crest Publishing: New Book Announcement

Introduction to Dynamical Systems and Geometric Mechanics

This text offers a comprehensive introduction to dynamics and mechanics from a modern geometric perspective, and contains several recent research results previously unpublished in any text.

For more information and a Google preview, readers should visit the Solar Crest Publishing website at http://www.solarcrestpublishing.com. For a limited time, readers can receive 30% off an order by using Coupon Code SIAM30.

Call for Proposals: SAMSI Summer Programs and Workshops

The Statistical and Applied Mathematical Sciences Institute has issued a call for proposals for summer programs and workshops that are focused on topics within the broad spectrum of new or recent research themes covered by SAMSI, to take place in the summer of 2013. Summer programs are short (one to two weeks) research programs that are consistent with SAMSI's core theme of bringing together statisticians, applied mathematicians, other mathematical scientists, and researchers in other disciplines; however, not every proposal needs to include all of these elements. Workshops are typically shorter (two to three days) and are focused on specific topics. Summer programs and workshops can act as seeds from which future year-long programs develop; such activities can help participants develop new SAMSI research themes without the workload required for year-long programs.

Proposals, which should be three to five pages in length and should include (1) a title and description of a proposed activity (e.g., whether it is a two-week summer program, a one-week summer program, or a two- to three-day workshop), (2) the names and affiliations of the organizing committee, (3) a rationale for and objectives of the program or workshop, (4) a list of leading researchers who are expected to be involved (commitments from specific individuals are encouraged but not required as part of the application process), and (5) a brief outline of how the program or workshop will be structured, should be sent to: summercompetition@samsi.info. The deadline for submission is July 27, 2012. All activities will take place at SAMSI, in Research Triangle Park, North Carolina; the final number of participants should be under 50.

Proposals will be evaluated by the SAMSI Directorate, members of which may contact prospective participants for further information. SAMSI plans to announce any accepted proposals for the summer of 2013 by the end of September 2012. Once a proposal is accepted, the SAMSI Directorate will work closely with the organizing committee on further development of the program or workshop, including budgeting, local arrangements, and the coordination of invitations. All the organizational arrangements will be made by SAMSI.

Further information about SAMSI can be found on the SAMSI website at http://www.samsi.info. Reports from past programs (including summer programs) can be downloaded from http://www.samsi.info/pgm-rpts.

2013 Budget

continued from page 2

proposals, a total of $9 million per year would be available. From this total, ASCR anticipates funding three or four centers, at about $2 million to $3.5 million each per year, with an additional nine teams funded at somewhat lower levels (each from $250,000 to $3.5 million per year). It is anticipated that the centers would be funded for five years, after which they could recompete.

The MMICCs are intended to address long-term mathematical problems arising from grand challenges in areas of interest to DOE. Such challenges include accelerating the discovery and design of new materials and chemistry for energy applications; developing methods for modeling and control of complex engineered systems, such as the U.S. power grid; methods for remediation of contaminants in subsurface flow and/or geologic sequestration of carbon dioxide; managing data at large-scale DOE facilities. Each raises a different set of mathematical challenges, from modeling to computational methods, optimization, and control.

Hitchcock describes the drive toward larger centers as motivated by the need for larger teams with diverse skills to tackle the more complex problems. "The trend is to do team-oriented research," he says, "but we continue to support individual PIs."

With mission-driven compute- and data-intensive challenges and significant changes in hardware, DOE applied mathematics needs to do more with the funding available. These centers could signal the start of major changes in the way the applied math program at DOE funds science.

■ ■ ■

What happens if the appropriations process produces less money than needed for the proposed research programs? Would the new programs and directions be derailed, waiting for future funds? Maybe. But more likely, reduced versions of the programs would be implemented through existing programs. In any event, the themes found in the budget are a roadmap to future federal investments.—*JMC*

An Uncertain Prognosis for Medicare Auctions: Part II

The first part of this article (May 2012) presented an auction design about to be implemented nationwide by the Centers for Medicare and Medicaid Services in awarding contracts for durable medical goods. A team of economists and mathematicians—Peter Cramton, Sean Ellermeyer, and Brett Katzman—pointed to flaws in the design. After a review of mathematical auction theory, the article offered a success story for comparison: the Federal Communications Commission's auctions of electromagnetic spectrum licenses in the 1990s.

By Erica Klarreich

The thinking behind the Centers for Medicare and Medicaid Services auction design is detailed in the *Federal Register* of April 10, 2007. The text makes no reference to results in the auction theory literature, and is peppered with sentences that start "We believe that," without offering scientific justification for those beliefs.

As described in the *Federal Register*, CMS considered four different auction structures. All choose the winners in the same way, starting with the lowest bid and working their way up the bids until there are enough providers to meet the projected demand. (To ensure a sufficient supply of the item in question, a CMS auction typically entails multiple winners.) The auctions differ in how they set the reimbursement price. In addition to the median of the winning bids (the method CMS ultimately chose), CMS considered using the minimum bid, the maximum winning bid, or a more complex adjusted average of the bids, a method it had tested in pilot auctions in 1999.

CMS discarded the adjusted average on the grounds that it made the reimbursement prices higher than the bids and rejected the minimum bid as not "reflective of the actual bids." CMS also rejected the maximum winning bid on the grounds that it would lead to payments that were higher than necessary, because some suppliers were willing to supply the item at a lower cost. The median, CMS wrote, is "representative of all the acceptable bids."

As explained in Part I, CMS made the bids non-binding: A winning bidder who is not happy with the reimbursement price does not have to accept a contract.

In its analysis of the four pricing rules, Brett Katzman observes, CMS incorrectly applied the principle of ceteris paribus, or "all other things being equal," when it assumed that the bids would stay the same no matter which auction design it used.

"The science of auctions—if not simple common sense—tells us that changing the pricing rule will change bidder strategies, and thus the comparisons CMS makes are useless," Katzman says. "Their reasoning was so bad that if my Intro Economics students used it, they would fail my class."

"The science of auctions—if not simple common sense—tells us that changing the pricing rule will change bidder strategies."

No Clear Strategy

In a median-price auction, it can be advantageous for a supplier to try to game the system by making a bid that's very far removed from his true costs. For example, a bidder with high costs might place an absurdly low bid, just to guarantee that he is included among the winners. His bid probably won't change the median price that much, and if the final price is too low to meet his costs, he can always walk away without signing the contract.

"A low-ball bid is a free option," comments Charles Plott, an economist at the California Institute of Technology.

To understand the ramifications of the median-price auction, Cramton, Ellermeyer, and Katzman set out to compute its Bayesian Nash equilibria, as described in Part I. In the real world, bidders will not necessarily use complex mathematics to identify their Bayesian Nash equilibrium strategies. However, Katzman says, an equilibrium is a proxy for where bidding should evolve to over time, as naive bidders gradually gain experience with an auction format and intuition about what strategies serve them well.

"If an auction has one good, solid, sensible equilibrium, that's a good sign that the auction will work well," Katzman says. "Otherwise, it's hard to tell how people will strategize, because even over time, they probably won't be able to figure out a profit-maximizing strategy."

In doing an equilibrium analysis of the CMS auctions, Cramton, Ellermeyer, and Katzman found themselves in uncharted waters. "No one had ever studied median-price auctions before, because, quite bluntly, no one was ever crazy enough to think they would work," Katzman says.

In this setting, finding a Bayesian Nash equilibrium amounts to looking for a bidding function—one that assigns a particular bid to each possible cost—such that if each bidder is using this function to determine his bid, then no bidder can increase his expected profit by switching to a different bid. Finding such a function boils down to solving a partial differential equation.

Using numerical methods, the research trio found that in the CMS auction design, infinitely many equilibria exist. "It's a really damning property of the Medicare auctions," Cramton says.

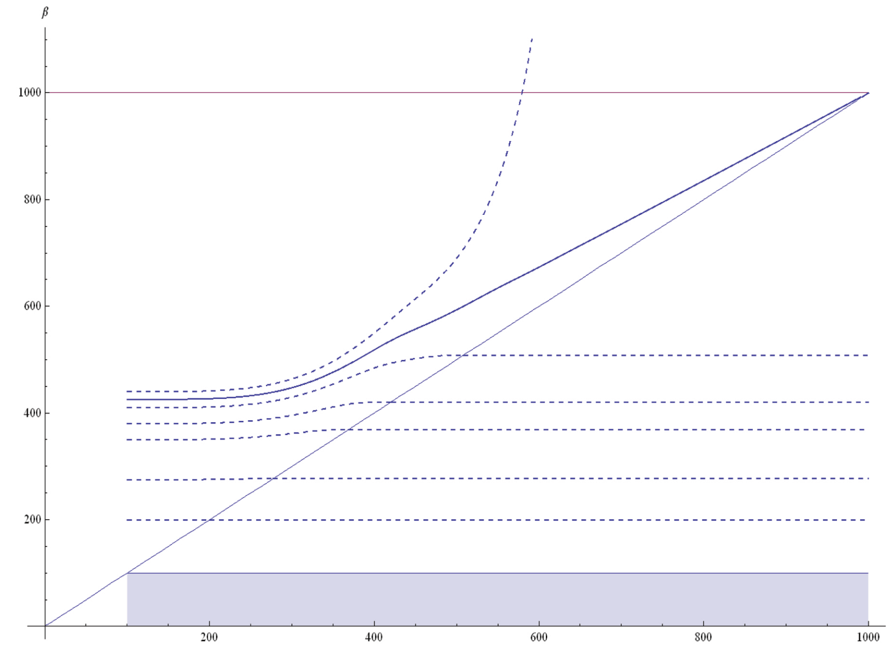

Figure 1. *Each of the above curves (except the diagonal line) represents an equilibrium bidding function in a model of the Medicare auctions with 16 bidders, whose costs* c *are uniformly distributed between \$100 and \$1000 and whose bids* β *are capped at \$1000. Any bidding function that lies entirely in the shaded area is also an equilibrium.*

Figure 1 shows the various families of equilibria that emerge from the team's model when 16 suppliers, whose costs are uniformly distributed between \$100 and \$1000, bid for seven contracts. In addition to the curves shown, any "low-ball" function whose graph lies entirely in the shaded area below \$100 is an equilibrium. In such a case, the median price is below all bidders' costs, and all will decline the contract; no individual can better his lot by unilaterally bidding over \$100, which will simply result in his losing the auction. Even the solid curve dividing the two dotted-line families of equilibria—in some sense the "nicest" of the equilibria—is not a satisfactory solution; the median is a price that some winners are likely to decline, which would lead to a shortage.

In any case, there's no reason to expect that bidders will gravitate toward that equilibrium, given the ever-present temptation to low-ball. In bidding experiments, Plott and colleagues at Caltech have shown that this temptation is all too real.

Poor Performance

To test the performance of the Medicare auction design experimentally, Plott and his colleagues asked groups of 12 or 16 volunteers to participate in auctions, with the incentive of modest cash awards for successful bids. Each participant was randomly assigned a cost for producing the (theoretical) item in question; after a practice period, the researchers held CMS-type auctions, in which each participant tried to maximize his profit.

As the theory predicts, bids were all over the map, with many high-cost bidders submitting low-ball bids. "You can see in the bidding that some people are trying to bid high enough to bring up the median without losing the auction, but without systematic coordination, they can't make that happen," Plott says. "When we repeated the auctions, the bids gradually converged to a very low price."

A very low price might sound great in view of ever-increasing medical costs, but the goal of an auction is to find not the lowest possible price, but rather the lowest sustainable price—the one that keeps providers in business and procures sufficient quantities of the items.

By these measures, the auctions conducted by Plott's team failed miserably. Only one in twenty succeeded in procuring the desired number of units, and one in five procured no units at all, as bidders low-balled and then walked away. And many low-cost bidders were shut out by higher-cost bidders who submitted low-ball bids.

"The results say fairly clearly that this auction architecture results in very poor performance in almost any dimension you could imagine," Plott says.

For comparison, Plott's team also tested a "clearing-price" auction, a well-studied design similar to that of the highly successful FCC spectrum auctions. In a clearing-price auction, in which bids are binding, the price is set at the bid of the lowest bidder who loses the auction. Bidding one's true cost is the "dominant" strategy—the best strategy no matter what the other bidders do.

The researchers found that for the most part, the volunteer bidders did figure out and implement this optimal strategy. Every one of the trial auctions succeeded in securing enough supply to meet the buyer's demand (automatically, as the bids were binding), and the low-cost bidders were usually the winners. In most cases, the final auction price was just slightly above the market clearing price—the price at which supply equals demand.

The simple expedient of making bids binding in the CMS auction would solve the problem of supply not meeting demand, and would also pretty much eliminate low-ball bidding—as, indeed, Plott's team found in experiments—as such bidders would run the risk of being held to their absurdly low bids. Yet even as this "fix" closed certain cans of worms, it would open others: In this case bidders would have to wrestle with the risks inherent in bidding at all in an auction in which they could ultimately be forced to accept a price lower than their bids.

In the case of binding median-price auctions, Cramton, Ellermeyer, and Katzman found that no equilibrium function exists. (More precisely, there is an infinite family of functions that satisfy the mathematical requirements to be equilibria, but the functions are non-monotonic, which makes no sense from an economics point of view.)

"In this setting, it's incredibly hard to decide how to bid," Katzman says.

Out of Business

So how have the actual CMS auctions performed? The pilot auctions in 1999 (which used the adjusted average method instead of the median bid to set the price) were marked by such wide price swings that CMS set upper and lower limits on allowable bids. "To put an upper limit on bids is not unusual, but to have to put a lower limit on bids when they want a low price should have been an indication to them that something is drastically wrong," Katzman says.

As might be expected, the 2009 auctions resulted in prices substantially lower than those in the earlier CMS fee schedules, and CMS touted the auctions as a notable success. It's hard for outsiders to assess how the auctions performed, however, because two years later, CMS has not revealed the bids. "There's a complete lack of transparency," says Cramton, who is using the Freedom of Information Act to try to elicit information about the auctions.

See **Medicare Auctions** *on page 6*