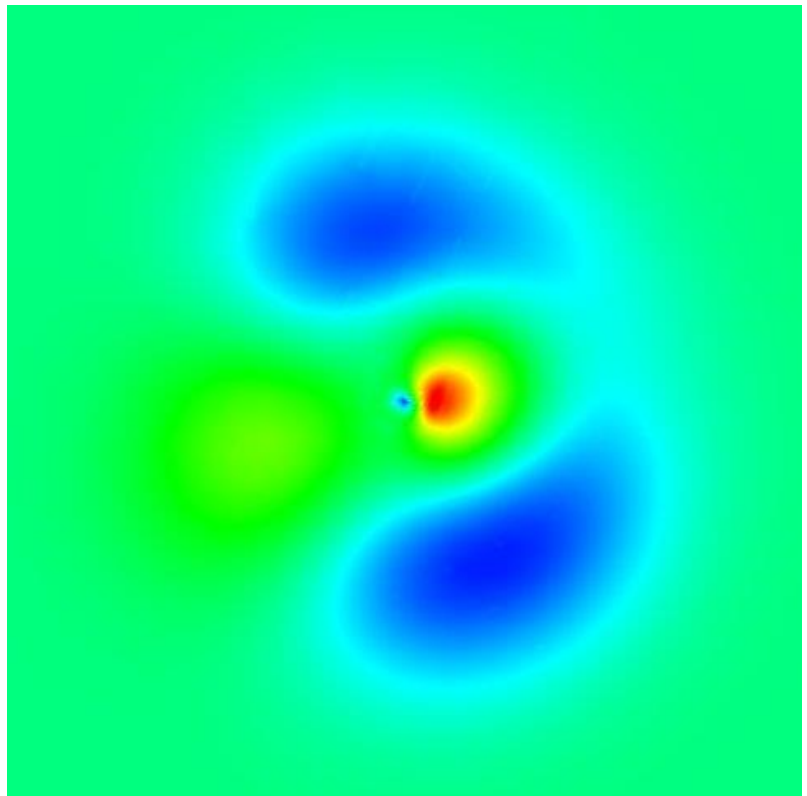


NISTIR 7994

<http://dx.doi.org/10.6028/NIST.IR.7994>

Applied and Computational Mathematics Division

Summary of Activities for Fiscal Year 2013



NISTIR 7994

Applied and Computational Mathematics Division

Summary of Activities for Fiscal Year 2013

Ronald F. Boisvert, Editor
*Applied and Computational Mathematics Division
Information Technology Laboratory*

<http://dx.doi.org/10.6028/NIST.IR.7994>

March 2014



U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Abstract

This report summarizes the technical work of the Applied and Computational Sciences Division of NIST's Information Technology Laboratory. Part I (Overview) provides a high-level overview of the Division's activities, including highlights of technical accomplishments during the previous year. Part II (Features) provides further details on five projects of particular note this year. This is followed in Part III (Project Summaries) by brief synopses of all technical projects active during the past year. Part IV (Activity Data) provides listings of publications, technical talks, and other professional activities in which Division staff members have participated. The reporting period covered by this document is October 2012 through December 2013.

For further information, contact Ronald F. Boisvert, Mail Stop 8910, NIST, Gaithersburg, MD 20899-8910, phone 301-975-3812, email boisvert@nist.gov, or see the Division's web site at <http://www.nist.gov/itl/math/index.cfm>.

Cover Visualization: Slice along the $z=0$ plane of the fourth wave function characterizing the interaction of two nonreactive polar RbCs molecules. Results computed using the system PHAML developed by the NIST Applied and Computational Mathematics Division. See page 64.

Acknowledgements: Thanks to Catherine Graham and Ginger White for assisting in the compilation of Parts III and IV of this document.

Disclaimer: Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Contents

PART I: OVERVIEW	1
Introduction	3
Highlights	5
<i>Technical Accomplishments</i>	5
<i>Technology Transfer and Professional Activities</i>	8
<i>Staff News</i>	9
<i>Recognition</i>	14
PART II: FEATURES	15
Approximating the Ising Partition Function	17
Compensating Operators and Stable Time Marching in Ill-Posed Nonlinear Evolution Equations	19
Single Photon Conversion Technology: Research to Commercialization	22
Analysis for Dynamic Metrology	26
A Framework for Reproducible Latent Fingerprint Enhancements	29
PART III: PROJECT SUMMARIES	33
Mathematics of Metrology	35
<i>Compensating Operators and Stable Time Marching in Ill-Posed Nonlinear Evolution Equations</i>	35
<i>Analysis for Dynamic Metrology</i>	35
<i>A Framework for Reproducible Latent Fingerprint Enhancements</i>	35
<i>Improved Time Delay Estimation Method in the Frequency Domain</i>	35
<i>Applied Hierarchical Control</i>	36
<i>Molecular Movies: Imaging Femtosecond Motion during Electrochemical Transitions</i>	37
<i>Stochastic Simulation in Chemical Spectroscopy</i>	38
<i>Computational Tools for Shape Measurement and Analysis</i>	39
<i>Computation of Shape Geodesics</i>	40
<i>Traceable Simulation of Magnetic Resonance Imaging</i>	41
<i>Modeling and Optimization in Cryobiology</i>	41
<i>Equilibrium and Stability of Drops on a Conical Substrate</i>	42
<i>Diffuse Interface Model Incorporating Interfacial Properties</i>	43
<i>Spectral-Galerkin Scheme to Study Ferroelectric Liquid Crystal Properties</i>	44
<i>Modeling Magnetic Fusion</i>	46
<i>Development of a New Solver for HVAC Simulation</i>	46
<i>Sustainable Design of Reinforced Concrete Structures</i>	48
<i>Modeling with Uncertainty Estimation of a Thickness-Shear MEMS Resonator</i>	48
<i>Using Quadratic Functions over Lines in Evolutionary Optimization</i>	49
<i>Separating Signal from Noise via the SVD</i>	50
<i>The Metrology of Supernova Light Curves</i>	50
<i>Sparse Low-rank Nonnegative Approximation of Interval Matrices</i>	51
Advanced Manufacturing	52
<i>Rheology of Dense Suspensions</i>	52

<i>Micromagnetic Modeling</i>	52
<i>OOOF: Finite Element Modeling of Material Microstructures</i>	53
<i>Solving the Diffusion Equation in Microstructures</i>	54
<i>Moving Grain Boundary Grooves under Stress</i>	54
<i>Morphological Stability</i>	55
<i>Inverse Method for Estimating Shear Stress in Machining</i>	55
<i>Model Selection for Fracture and Fatigue Failure Data of Engineering Materials</i>	56
<i>Structural Design Allowables for Composites</i>	57
High Performance Computing and Visualization	59
<i>A Dynamic Computational Phantom for RF Propagation in Body Area Networks</i>	59
<i>Rheology of Dense Suspensions</i>	59
<i>Modeling and Visualization of Cement Paste Hydration and Microstructure Development</i>	61
<i>High Precision Calculations of Fundamental Properties of Few-Electron Atomic Systems</i>	62
<i>Nano-structures, Nano-optics, and Controlling Exciton Fine Structure</i>	63
<i>Parallel Adaptive Refinement and Multigrid Finite Element Methods</i>	64
<i>Texture Compression Evaluation and Optimization</i>	65
<i>Declarative 3D Graphics</i>	66
<i>Optical Characterization of Immersive 3D Displays</i>	67
<i>Visualization for Measurement Science for Complex Information Systems</i>	68
Mathematical Knowledge Management	70
<i>Digital Library of Mathematical Functions</i>	70
<i>Mathematical Knowledge Representation</i>	71
<i>Visualization of Complex Functions Data</i>	72
<i>Standard Reference Tables on Demand</i>	74
<i>Digital Repository of Mathematical Formulae</i>	75
<i>Eigenfunction Expansions for Special Functions and Orthogonal Polynomials</i>	77
Quantum Information	80
<i>Single Photon Conversion Technology: Research to Commercialization</i>	80
<i>Quantum Information Science</i>	80
<i>Quantum Computing Benchmarks</i>	81
<i>Quantum State Estimation Theory and Experiment</i>	82
<i>Random Number Generation based on Bell Inequality Violation</i>	83
<i>Tamper-Resistant Cryptographic Devices based on Quantum Mechanics</i>	84
<i>Post-Quantum Cryptography</i>	85
<i>High-Speed Low Density Parity Codes for Quantum Key Distribution</i>	85
<i>Simulating Quantum Field Theories on Quantum Computers</i>	86
<i>Circuit Obfuscation and Synthesis</i>	87
<i>Quantum Adiabatic Optimization</i>	88
Foundations of Measurement Science for Information Systems	89
<i>Systemic Risks/Benefits of Interconnectivity</i>	89
<i>Examining the Gromov Curvature of Networks in Time</i>	90
<i>An Improved Feedback Vertex Set Heuristic</i>	90
<i>Broadcast and Spread of Information in Complex Networks</i>	91
<i>An Algebraic Formulation for the Analysis and Visualization of Network Graphs</i>	92

<i>Security Risk Analysis of Enterprise Networks using Attack Graphs</i>	93
<i>Combinatorial Testing</i>	94
<i>Coverage and Energy Optimization in Mobile Sensor Networks</i>	95
<i>A Dynamic Computational Phantom for RF Propagation in Body Area Networks</i>	96
<i>Evaluation and Mitigation Strategies for Cross-Interference between Multiple Body Area Networks</i>	97
PART IV: ACTIVITY DATA	99
Publications	101
<i>Appeared</i>	101
Refereed Journals	101
Journal of Research of NIST	102
Books	102
Conference Proceedings	102
Technical Magazine Articles	105
Technical Reports	105
<i>Accepted</i>	105
<i>In Review</i>	106
<i>Invention Disclosures</i>	106
Presentations	107
<i>Invited Talks</i>	107
<i>Conference Presentations</i>	110
Web Services	112
Software Released	112
Conferences, Minisymposia, Lecture Series, Courses	112
<i>MCS D Seminar Series</i>	112
<i>Courses/Shortcourses Taught</i>	113
<i>Conference Organization</i>	113
Other Professional Activities	115
<i>Internal</i>	115
<i>External</i>	115
Grants Awarded	117
External Contacts	117
PART V: APPENDIX	119
Staff	121
Glossary of Acronyms	124

Introduction

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. The NIST Laboratory program is broad-ranging, with research efforts in physics, electrical engineering, materials science, chemistry, bioscience, engineering, fire research, and information technology.

The Information Technology Laboratory (ITL) is one of six major laboratories and user facilities at NIST. ITL seeks to (a) accelerate the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure; (b) advance measurement science through innovations in mathematics, statistics, and computer science; and (c) conduct research to develop the measurements and standards infrastructure for emerging information technologies and applications.

The Applied and Computational Mathematics Division (ACMD) is one of six technical Divisions in ITL. ACMD provides leadership within NIST in the use of applied and computational mathematics to solve science and engineering problems arising in measurement science and related applications. In that role ACMD staff members

- perform research and development in applied mathematics and computer science and engineering, including analytical methods, numerical and symbolic algorithms, advanced computing and communications architectures and applications, and high performance scientific visualization;
- engage in peer-to-peer collaborations in the application of mathematical and computational technologies to NIST problems;
- develop and disseminate mathematical reference data, software, and related tools; and
- work with internal groups and external organizations to develop standards, test procedures, reference implementations, and other measurement technologies for advanced scientific computation on current and future architectures.

Division staff is organized into four groups:

Mathematical Analysis and Modeling Group (*Timothy Burns, Leader*)

Performs research and maintains expertise in applied mathematics, mathematical modeling, and numerical analysis for application to measurement science.

Mathematical Software Group (*Michael Donahue, Leader*)

Performs research and maintains expertise in the methodology and application of mathematical algorithms and software in support of computational science within NIST as well as in industry and academia.

Computing and Communications Theory Group (*Ronald Boisvert, Acting Leader; Isabel Beichl and Xiao Tang, Project Leaders*)

Performs research and maintains expertise in fundamental mathematics, physics, and measurement science necessary to enable the development of future computing and communications systems.

High Performance Computing and Visualization Group (*Judith Terrill, Leader*)

Performs research and maintains expertise in the methodologies and tools of high performance scientific computing and visualization for use in measurement science.

The technical work of the Division is organized into six thematic areas; these are described in the sidebar. Project descriptions in Section III of this document are organized according to these broad themes.

Division Thematic Areas

Mathematics of Metrology. Mathematics plays an important role in the science of metrology. Mathematical models are needed to understand how to design effective measurement systems, and to analyze the results they produce. Mathematical techniques are used to develop and analyze idealized models of physical phenomena to be measured, and mathematical algorithms are necessary to find optimal system parameters. Finally, mathematical and statistical techniques are needed to transform measured data into useful information. The goal of this work is to develop fundamental mathematical methods and analytical tools necessary for NIST to continue as a world-class metrology institute, and to apply them to critical measurement science applications.

Advanced Manufacturing. Delivering technical support to the nation's manufacturing industries as they strive to out-innovate and out-perform the international competition has always been a top priority at NIST. This has also emerged as a major White House priority in recent years, in which NIST is playing an increasingly central role. Mathematical modeling, computational simulation, and data analytics are key enablers of emerging manufacturing technologies. This is most clearly evident in the Materials Genome Initiative, an interagency program with the goal of significantly reducing the time from discovery to commercial deployment of new materials through the use of modeling, simulation, and informatics. ACMD's role in advanced manufacturing centers on the development and assessment of modeling and simulation tools, with emphasis on uncertainty quantification, as well as support of NIST Laboratory efforts in such areas as nanomanufacturing, smart manufacturing, and materials modeling.

High Performance Computing and Visualization. Computational capability is advancing rapidly, with the result that modeling and simulation can be done with greatly increased fidelity (e.g., higher resolution, more complex physics). However, developing large-scale parallel applications remains highly challenging, requiring expertise that scientists rarely have. In addition, the hardware landscape is changing rapidly, so new algorithmic techniques must constantly be developed. We are developing and applying such facilities and expertise for application to NIST problems. Computations and laboratory experiments often produce large volumes of scientific data, which cannot be readily comprehended without some form of visual analysis. We are developing the infrastructure necessary for advanced visualization of scientific data, including the use of 3D immersive environments and applying this to NIST problems. One of our goals is to develop the 3D immersive environment into a true interactive measurement laboratory.

Mathematical Knowledge Management We work with researchers in academia and industry to develop technologies, tools, and standards for representation,

exchange, and use of mathematical data. Of particular concern are semantic-based representations which can provide the basis for interoperability of mathematical information processing systems. We apply this to the development and dissemination of reference data for applied mathematics. The centerpiece of this effort is the Digital Library of Mathematical Functions, a freely available interactive and richly linked online resource, providing essential information on the properties of the special functions of applied mathematics, the foundation of mathematical modeling in all of science and engineering.

Quantum Information. An emerging discipline at the intersection of physics and computer science, quantum information science (QIS) is likely to revolutionize science and technology in the same way that lasers, electronics, and computers did in the 20th century. By encoding information into quantum states of matter, one can, in theory, exploit the seemingly strange and counter-intuitive behavior of quantum systems to enable phenomenal increases in information storage and processing capability, as well as communication channels with extremely high levels of security. Although many of the necessary physical manipulations of quantum states have been demonstrated experimentally, scaling these up to enable fully capable quantum computers remains a grand challenge. We engage in (a) theoretical studies to understand the power of quantum computing, (b) collaborative efforts with the multi-laboratory experimental quantum science program at NIST to characterize and benchmark specific physical implementations of quantum information processing, and (c) the development and assessment of technologies for quantum communication.

Foundations of Measurement Science for Information Systems. Modern information systems are astounding in their complexity. Software applications are built from thousands of interacting components. Computer networks interconnect millions of independently operating nodes. Large-scale networked applications provide the basis for services of national scope, such as financial transactions and power distribution. In spite of our increasing reliance on such systems, our ability to build far outpaces our ability to secure. Protocols controlling the behavior of individual nodes lead to unexpected macroscopic behavior. Local power anomalies propagate in unexpected ways leading to large-scale outages. Computer system vulnerabilities are exploited in viral attacks resulting in widespread loss of data and system availability. The stability of our critical infrastructure is simply unknown. Measurement science has long provided a basis for the understanding and control of physical systems. Such deep understanding and insight is lacking for complex information systems. We seek to develop the mathematical foundations needed for a true measurement science for complex networked information systems.

Highlights

In this section we identify some of the major accomplishments of the Division during the past year. We also provide news related to ACMD staff.

Technical Accomplishments

ACMD has made significant technical progress on many fronts during the past year. Here we highlight a few notable technical accomplishments with significant impact. Further details are provided in Part II (Features) and Part III (Project Summaries).

Mathematics of Metrology. An important focus of ACMD is the development of mathematical methods and tools of use in metrology, and their application to modeling and analysis problems at NIST. Our work in this area is very broad. The applications we considered this year range from the interpretation of data from measurements of femtosecond-scale electrochemical transitions to supernova light, and the modeling of phenomena from liquid crystals to building ventilation systems. In the process we develop fundamental mathematical tools such as novel time-delay estimation methods, stable time-marching methods for ill-posed nonlinear evolution equations, and special-purpose optimization methods.

Among the new metrological challenges that we are working on include dynamic metrology, the measurement of time varying quantities, which is requiring specialized approaches to signal analysis. While our efforts are focused on the measurement of time-varying waveforms for communications applications, the same mathematical issues are now turning up in the measurement of time-varying pressure, force, and torque (see page 26). Another novel measurand is shape, which is of interest in characterizing, for example, cell colonies in microscope images, cancer indicators in medical imagery, or microstructures in material micrographs. We are cooperating with the ITL Statistical Engineering Division in a NIST Innovations in Measurement Science (IMS) project to develop techniques and tools for shape metrology with application to NIST problems (see pages 39 and 40).

Another growth area for ACMD is metrology for modeling and simulation. We seek to develop techniques and tools for verification, validation, and uncertainty analysis that enables a quantitative understanding of the uncertainty in results produced by computational simulation. Reference problems are an important tool for verification, enabling intercomparison of modeling codes. We continue to develop new such problems for the field of micromagnetics (see page 52), and this year we unveiled an online repository of reference problems useful for comparison of adaptive grid solvers for partial differential equations (see page 64). An important part of physical metrology is the concept of traceability of a measurement to a reference standard. This year we initiated a project to create SI¹-traceable simulations for magnetic resonance imaging (see page 41).

Advanced Manufacturing. NIST work in measurements, standards and technologies are an important enabler of innovation in the manufacturing sector. In the last few years NIST has been participating in the interagency Materials Genome Initiative (MGI) within the President's Advanced Manufacturing Partnership unveiled in 2011. The MGI seeks to promote the widespread use of modeling and simulation and data informatics to greatly reduce the time and cost from materials discovery and deployment. ITL works closely with the NIST Material Measurement Laboratory to carry out NIST's work under the MGI. ACMD's role is principally in two areas: the development and assessment of modeling and simulation software, and the development of techniques and tools for the quantification of uncertainty in materials models and simulations. ACMD's OOMMF (page 52) and OOF (page 53) projects are partially supported by MGI funding, for example. In addition, we have developed alliances with several external partners to advance Division engagement with the MGI. Researchers at the University of California at San Diego are developing a graphical processing unit (GPU) version of OOMMF to enable cost-effective high resolution micromagnetics simulations. The Institute of Mathematics and Its Applications (IMA) at the University of Minnesota has undertaken a NIST-supported project on uncertainty quantifica-

¹ International System of Units, see <http://physics.nist.gov/cuu/Units/>

tion (UQ) in molecular dynamics simulations of resins used in composite materials. As part of that work, the IMA has engaged a postdoc who is spending part of his tenure at Boeing, where he is learning industrial applications first-hand. On December 16-17, 2013, the IMA hosted a NIST-supported workshop entitled *Uncertainty Quantification in Materials Modeling*²; some 30 researchers representing both the UQ and materials modeling community attended. Follow-on is planned.

Finally, on December 3, 2013 NIST announced³ that it has selected a consortium led by Northwestern University to establish a new NIST-sponsored center of excellence for advanced materials research. The new Center for Hierarchical Materials Design (CHiMaD), whose other partners include the University of Chicago and Argonne National Laboratory, will be funded in part by a \$25 million award from NIST over five years. We anticipate many opportunities to collaborate with CHiMaD researchers in the next few years.

High Performance Computing and Visualization. ACMD provides leadership within NIST in the application of high performance computers to the solution of metrology problems of importance to the NIST labs. A good example is our work in the modeling of the rheology of dense suspensions, in which our simulations, run on the Blue Gene/Q system at the Argonne National Laboratory Leadership Computing Facility, are being used to develop novel designs for rheometers as well as standard reference materials used to calibrate them (see page 59).

ACMD continues to set new accuracy records for computations of non-relativistic ground state energies of few electron atomic systems. Fundamental understanding of atomic systems is necessary for a wide variety of applications including material design, drug discovery, and providing a testbed for quantum theory. Despite their small size, atomic systems present enormous challenges for scientists hoping to compute their properties from first principles. These difficulties have resulted in much of our computational infrastructure being predicated on simplifying assumptions. In ACMD we have taken a different approach. For several years we have invested in developing the foundational analytical and numerical machinery to solve the few-electron Schrödinger system with no approximations other than the truncation of infinite series. This investment has resulted in several extreme-accuracy firsts in the world of computational atomistics. In FY 2013, ACMD researchers computed the ground-state energy of the four-electron Beryllium atom to eight digits of accuracy using an expansion with 70000 unknowns to represent the solution. By extending these results we have been able to perform the most accurate computations ever done – eight digits of accuracy – of the entire isoelectronic series up through atomic number 113. The four-electron case is particularly exciting as, due to the ACMD formalism, higher electron systems will present no new analytical difficulties. These results are being prepared for publication (see page 62).

Visual-based analysis is an indispensable tool for the interpretation of both large-scale simulation results and massive collections of measured data. For some time we have been working to develop 3D immersive visualization environments into virtual measurement laboratories. This requires a deep understanding of the uncertainty introduced by the visualization system itself. To this end we have undertaken a project with the NIST Physical Measurement Laboratory to perform optical characterization of immersive 3D displays (see page 67).

Mathematical Knowledge Management. In a world where technical communication is increasingly done online, technologies, tools, and standards for the representation, exchange and use of mathematical data are critical. The current state-of-the-art is less than ideal, and we are trying to improve it. An important aspect is the generation of content that conforms to MathML, the W3C standard for the representation of math on the Web. LaTeXML, developed by ACMD, has become a popular tool for converting documents coded in the popular mathematical typesetting system LaTeX to MathML (see page 71). This is a surprisingly challenging problem, for which ACMD has developed considerable expertise.

At NIST, the main application for LaTeXML has been the generation of content for the NIST Digital Library of Mathematical Functions (DLMF), an online reference work on the properties of the special functions of applied mathematics, which was released in 2010. Already a popular online resource,

² http://www.ima.umn.edu/2013-2014/SW12.16-17.13/?event_id=SW12.16-17.13

³ <http://www.nist.gov/mml/coe-120313.cfm>

the DLMF is being actively maintained and continues to be developed. This year, for example, all of the interactive 3D visualizations of mathematical functions in the DLMF have been converted to WebGL, a JavaScript API for rendering interactive 3D graphics objects in a web browser without the use of a plugin (see page 72). The new visualizations will be released soon. Another capability under active development is a tool for generating tables on demand with carefully characterized uncertainty (see page 74). A major blow was dealt to the DLMF project this year with the passing of its esteemed Mathematics Editor, Frank W. J. Olver (see page 9). Considerable work has gone into the development of plans to ensure continued strong support for the project (see page 70).

Quantum Information. Our work in quantum information science is focused in three main areas: (a) theoretical understanding how quantum resources can be used to greatly increase our ability to perform information processing tasks, (b) techniques for characterizing the results of quantum-based measurements, e.g., quantum state tomography and quantum computer benchmarking, and (c) demonstration and characterization of systems for quantum communications.

This year ACMD theorists developed new and effective analysis methods for determining the extent to which experiments violate classicality assumptions, thus verifying fundamental notions of quantum theory (see page 80). Such Bell tests are still extraordinarily difficult to perform; most require unwanted assumptions (“loopholes”) that cast doubt on their validity. ACMD is working with the NIST Physical Measurement Laboratory on a NIST Innovations in Measurement Science project, which will attempt to close such loopholes. Entangled photons violating the Bell test, which would certify that no one in the universe could have known their state before measurement, will be used as a physical source of randomness, ultimately feeding the NIST Random Number Beacon under development by the ITL Computer Security Division (see page 83).

In another effort, we have developed new insight in the use of quantum mechanics to construct an important class of tamper-resistant devices called one-time memories. Such memories represent an important primitive that enables powerful applications in computer security, such as one-time programs. We find that one-time memories *cannot* exist in a world that is fully classical or fully quantum; but, surprisingly, one-time memories *can* be built in a world that is *partly* quantum (see page 84).

The need for reliable and efficient single photon detectors suitable for application in long-distance quantum communications has led ACMD scientists to create and improve single photon frequency upconversion technology. ITL is now a world leader in the development and application of this technique, as evidenced by the publication of a survey of the group’s work over the past five years in the highly cited journal *Physics Reports*. The team has also been successful in working to transfer ACMD-developed technology to small businesses through the NIST Small Business Innovative Research (SBIR) Program. The team’s pioneering work is also providing the basis for a new initiative at the Defense Advanced Research Projects Agency (DARPA) (see page 22).

Foundations of Measurement Science for Information Systems. Abstract networks, also known in mathematics as graphs, provide an important basis for mathematical models in many fields, including computer science (information and software), engineering (the Internet and the power grid), biology (protein interactions and food webs), and the social sciences (social networks). In ACMD, we are studying metrics for characterizing the structure of large networks, with the aim to understand how structure influences dynamics of processes operating on networks. This year our work in the development of computational algorithms for network problems yielded significant results for the study of fundamental models in physics. Using insights from combinatorics and graph theory we developed a completely new, and highly efficient, method for approximating the partition function of the Ising model (see page 17). While originally developed as a model of the statistical mechanics of magnetic systems, many difficult computational problems in material science, bioscience, and computer science can be formulated as special instances of the Ising model.

For the last three years ACMD has had a collaboration with Bell Labs to study the geometrical properties of large-scale networks. The third of a series of workshops on this topic was held on October

Table 1. Approximate number of downloads of selected division software packages during CY 2013

Package	Description	Downloads
JAMA	Linear algebra in Java	23 700
OOMMF	Modeling of nano-magnetic phenomena	11 000
TNT	Linear algebra using C++ templates	2 800
OOF	Modeling materials with complex microstructure	1 100
Ngraph	Basic graph algorithms; web crawler	900
spblas	Sparse basic linear algebra components	800
f90gl	Fortran 90 interface to OpenGL graphics	675
PHAML	Parallel adaptive solution of partial differential equations	360

25, 2013. The *Bell Labs – NIST Workshop on Large-scale Networks*⁴, which took place in Murray Hill, NJ, had 28 participants (8 from NIST). Discussion topics included the measurement of key geometrical properties (e.g., dimension and curvature), characteristics of flow influenced by such features, and effective computation and approximation methods for such problems.

This year we forged a new alliance with the Santa Fe Institute (SFI) to help deepen our connection to the complex systems research community. With funding provided from a NIST grant, the SFI will be holding a series of workshops in the general areas of network science, biology-inspired computing, and computer security. The first such workshop, *Structure, Statistical Inference, and Dynamics in Networks: From Graphs to Rich Data*⁵, which was held on May 6-9, 2013 in Santa Fe, attracted 44 participants (5 from ACMD). The second, *Deep Computation in Statistical Physics*⁶, held on August 8-10, 2013, had 22 participants (3 from ACMD).

Technology Transfer and Professional Activities

The volume of technical output of ACMD remains high. During the last 18 months, Division staff members were (co-)authors of 34 articles appearing in peer-reviewed journals and 44 papers in conference proceedings. Thirteen additional papers have been accepted for publication, while 22 others are undergoing review. Division staff members gave 66 invited technical talks and presented 49 others in conferences and workshops.

ACMD continues to maintain an active Web site with a variety of information and services, including the Digital Library of Mathematical Functions, the Guide to Available Mathematical Software, the Matrix Market, and the SciMark Java benchmark. During calendar year (CY) 2013, the division web server satisfied more than 4.6 million requests for pages from more than 382,000 distinct hosts. In total, there have been more than 354 million “hits” on ACMD Web servers since they went online as NIST’s first web servers in 1994. The individual software packages that we produce and distribute also continue to see very high usage. Table 1 lists download counts for some of our most popular ones. Another indication of the successful transfer of our technology is references to our software in refereed journal articles. For example, our OOMMF software for nano-magnetic modeling was cited in 150 such papers published in CY 2013 alone (more than 1,590 such papers have been identified since 2001).

Members of the Division are also active in professional circles. Staff members hold a total of 16 editorial positions in peer-reviewed journals. This year Isabel Beichl completed her second term as Editor-in-Chief of the IEEE/AIP publication *Computing in Science & Engineering*. ACMD faculty appointee Dianne O’Leary serves at Editor-in-Chief of the *SIAM Journal on Matrix Analysis and Applications*. Staff members are also active in conference organization, serving on 25 organizing/steering/program committees.

⁴ <http://ect.bell-labs.com/who/iis/research/workshops/NIST-BellLabsWorkshopOct25-2013x.pdf>

⁵ <http://www.santafe.edu/gevent/detail/science/1175/>

⁶ <http://www.santafe.edu/gevent/detail/science/1176/>

Service within professional societies is also prevalent among our staff. For example, Ronald Boisvert completed his third (and final) term as Co-Chair of the Publications Board of the Association for Computing Machinery (ACM). In this role he served as a member of the ACM Council, the association's board of directors. In addition, staff members serve on committees of the IEEE Computer Society and the Mathematical Association of America. Staff members are also active in a variety of working groups. For example, Ronald Boisvert and Andrew Dienstfrey serve as members of the International Federation for Information Processing (IFIP) Working Group 2.5 on Numerical Software, Donald Porter is a member of the Tcl Core Team, Bruce Miller is a member of W3C's Math Working Group, Kamran Sayrafian is a member of the IEEE 802.15 Working Group on Wireless Personal Area Networks, Vladimir Marbukh is a member of the Network Complexity Research Group of the Internet Research Task Force (IRTF), and Sandy Ressler is a member of the Declarative 3D for the Web Architecture Community Group. Judith Terrill represents NIST on the High End Computing Interagency Working Group of the Federal Networking and Information Technology Research and Development (NITRD) Program. Robert Bohn is Co-Chair of the NITRD Program's Faster Administration of Science and Technology Education and Research (FASTER) Community of Practice.

For further details, see Section IV, Activity Data.

Staff News

The past year saw many staffing changes. Among these are the following.

Arrivals

Sean Colbert-Kelly began his term as a NIST/NRC Postdoctoral Associate in ACMD in January 2013. Colbert-Kelly received a Ph.D. in Mathematics from Purdue University in 2012. At Purdue he undertook a theoretical and computational analysis of a Ginzburg-Landau type energy for Smectic C* Liquid Crystals. At NIST he will be continuing this work with Geoffrey McFadden studying dynamical properties of vortices.

Ginger White joined ACMD in February 2013 as Group Secretary for the Mathematical Modeling and Analysis and Mathematical Software Groups. White comes to ACMD from the National Library of Medicine at the NIH where she served as a library technician. She has had previous experience as a technical writer with the USDA and as a broadcast journalist with the US Army.

Formerly a senior research scientist at the Courant Institute of Mathematical Sciences at New York University, **Zydrunas Gimbutas** joined ACMD in Boulder in July 2013. Gimbutas, who received a Ph.D. in Applied Mathematics from Yale University in 1999, has more than 15 years of experience designing, analyzing and implementing fast numerical algorithms of applied analysis for computational acoustics and electromagnetics, quadratures for singular functions, and scientific computing. Before his appointment at Courant, Gimbutas served for five years as a research scientist at MadMax Optics, Inc.

In July 2013 **Michael Cromer**, a postdoctoral scholar at the University of California at Santa Barbara, joined ACMD as a NIST/NRC Postdoctoral Associate. Cromer received a Ph.D. in Applied Mathematics from the University of Delaware in 2011, where he wrote a thesis on models of wormlike micellar mixtures. At NIST Cromer will work with Geoffrey McFadden on the modeling and simulation of shear thickening fluids.

Richard La, Associate Professor of Electrical and Computer Engineering and the Institute for Systems Research at the University of Maryland, began a Guest Researcher appointment in ACMD in July 2013. La, who received a Ph.D. in EECS from the University of California at Berkeley in 2000, will be conducting research in network science, with applications to computer security.

Paulina Kuo joined ACMD in September 2013 after spending two years with ACMD as a guest researcher supported by the Joint Quantum Institute. Kuo received undergraduate degrees in Physics and Materials Science from MIT. In 2008 she received a PhD in Applied Physics from Stanford University. She also served as a NIST/NRC Postdoctoral Associate in the NIST Physical Measurement Laboratory.

An expert in nonlinear optics, Kuo will be contributing to the Division's experimental efforts in quantum communications.

Michael Mascagni, Professor of Computer Science at Florida State University, began a Faculty Appointment in ACMD in September 2013. Mascagni received Ph.D. in Applied Mathematics from the Courant Institute at NYU in 1987, and has held appointments at NIH, the Supercomputing Research Center and the University of Southern Mississippi. At FSU he holds joint appointments in the Mathematics and the Scientific Computing Departments. His research interests include computational science, numerical analysis, Monte Carlo methods, and random number generation. At NIST he will be contributing to efforts in materials modeling and parallel computing.

Yvonne Kemper began a stay in ACMD as a NIST/NRC Postdoctoral Associate in December 2013. She received a Ph.D. in mathematics from the University of California at Davis in 2013, where she wrote a thesis on structural measurements of simplicial complexes and convex polytopes. At NIST she will be working with Isabel Beichl on approximating flow and chromatic polynomials of big data networks.

Departures

Agnes (Abbie) O’Gallagher of ACMD retired in November 2012 after 27 years of service at the NIST Boulder Labs. During her career at NIST O’Gallagher provided support for ACMD efforts in cryocooler modeling, DNA sequence alignment, and CT scanner modeling. She was also an active member of ITL’s Diversity Committee, where she organized the very successful ITL Diversity Book Club.

Adele Peskin, a long-standing member of ACMD’s High Performance Computing and Visualization Group in Boulder, has transferred to ITL’s Software and Systems Division. There she will continue work, started during her tenure in ACMD, on the analysis of imagery from biology and medicine.

Asha Nurse completed her term in ACMD as an ARRA Postdoctoral Fellow in February 2013. At NIST she worked with Geoffrey McFadden on an analysis of bubble motion and size variation during thermal migration with phase change, as well as the equilibrium and stability of drops on a conical substrate with application to tissue engineering. She continues her affiliation with NIST as a guest researcher.

Yong-Su Kim, who joined ACMD in March 2012 as a guest researcher from the Pohang University of Science and Technology in South Korea, returned to Korea in March 2013. An expert in quantum optics, Kim contributed his expertise to ITL’s quantum communications project in the area of frequency up-conversion technology.

Elizabeth Moseman, former NIST/NRC Postdoctoral Associate, departed NIST for a permanent position at the National Security Agency in the spring of 2013. At NIST, Moseman worked on algorithms for computing properties of large-scale graphs.

Amada Streib and **Noah Streib**, NIST/NRC Postdoctoral Associates in ACMD departed in August 2013, accepting positions at the Institute for Defense Analysis’ Center for Computing Sciences in Bowie, MD. The Streibs each received Ph.D.’s in the Algorithms, Combinatorics and Optimization program at Georgia Tech. At NIST they worked with Isabel Beichl on novel graph theoretic methods for efficient simulation of the Ising model of computational physics.

Ismet Sahin completed his term in ACMD as an ARRA Senior Fellow in April 2013. At NIST Sahin worked with Anthony Kearsley on evolutionary optimization algorithms, as well as applications to waveform time delay estimation algorithms that are used in seismology, radar, sonar, and biomedical science.

Daniel Kaslovsky, recipient of an NSF Postdoctoral Fellowship for Transformative Computational Science using CyberInfrastructure, who was carrying out his research in ACMD in Boulder, accepted a permanent position at Seagate Technology in Longmont, Colorado.

Table 2. Student Interns in ACMD

Name	Institution	Type	Mentor	Project
Philip Lenzini	Univ. of Colorado	G PREP	E. Knill	Statistics for quantum information
Adam Meier	Univ. of Colorado	G PREP	E. Knill	Quantum computer simulation
Rebecca Mitchell	Univ. of Colorado	G PREP	B. Alpert	Numerical linear algebra
Michael Mullan	Univ. of Colorado	G PREP	E. Knill	Quantum computing theory
James Van Meter	Univ. of Colorado	G PREP	E. Knill	Quantum measurement of space-time
Yanbao Zhang	Univ. of Colorado	G PREP	E. Knill	Tests of local realism
Hamza Attak	ISIMA (France)	G FGR	J. Terrill	Visualization algorithms
Martina Barbi	U. Bologna (Italy)	G FGR	K. Sayrafian	RF propagation in body-area networks
Styvens Belloge	ISIMA (France)	G FGR	J. Terrill	Visualization in computer security
Yannick Congo	ISIMA (France)	G FGR	S. Langer	Finite element analysis of microstructure
Deyan Ginev	Jacobs U. (Germany)	G FGR	B. Müller	Semantics of mathematical documents
Gregory Rami	ISIMA (France)	G FGR	J. Terrill	Impact of fire on building structures
Earl Bellinger	SUNY Oswego	G NPSC	J. Terrill	Data mining
Bryan Gard	Louisiana State Univ.	G NPSC	E. Knill	Quantum measurement analysis
Adam Keith	Univ. of Colorado	G NSF	E. Knill	Quantum measurement analysis
Michael Baume	Univ. of Maryland	G DGR	S. Jordan	Analysis of quantum algorithms
Rehab Al Ammary	Montgomery College	U SURF	A. Gueye	Identifying critical links in networks
Michael Baeder	Harvey Mudd College	U SURF	H. Cohl	Hypergeometric orthogonal polynomials
Kevin Keller	Univ. of Maryland	U SURF	J. Terrill	Analysis of early-age cement hydration
Andrea Rommal	Muhlenburg College	U SURF	A. Mink	Quantum randomness amplification
Rebekah Wheatley	Johns Hopkins Univ.	U SURF	H. Cohl	Functions in hyperspherical geometry
Janelle Williams	Virginia State Univ.	U SURF	H. Cohl	Web resources for special functions
Luis Catacora	Univ. of Maryland	U DGR	J. Terrill	Immersive visualization for HydratiCA
Ajay Kannan	Dartmouth College	U Vol.	S. Langer	Image processing
Philbert Hwang	Poolesville H. S.	HS SHIP	H. Cohl	Hypergeometric orthogonal polynomials
Amolak Nagi	Walt Whitman H. S.	HS SHIP	S. Ressler	Web-based visualizations
Alicia Ouyang	River Hill H. S.	HS Vol.	J. Terrill	Information visualization using D3

Legend	<i>G</i>	<i>Graduate student</i>	<i>PREP</i>	<i>Professional Research Experience Program (Boulder)</i>
	<i>U</i>	<i>Undergraduate</i>	<i>FGR</i>	<i>Foreign Guest Researcher</i>
	<i>HS</i>	<i>High school</i>	<i>NPSC</i>	<i>National Physical Sciences Consortium Fellow</i>
			<i>NSF</i>	<i>National Science Foundation Fellow</i>
			<i>DGR</i>	<i>Domestic Guest Researcher</i>
			<i>SURF</i>	<i>Summer Undergraduate Research Fellowship</i>
			<i>SHIP</i>	<i>Summer High school Internship Program</i>
			<i>Vol.</i>	<i>Volunteer</i>

Students

During FY 2013 ACMD was able to support the work of 27 student interns, including 16 graduate students, eight undergraduates, and three high school students. See Table 2 for a complete listing.

ACMD staff members are quite active in the education of graduate students, serving both as Ph.D. advisers and as members of thesis committees. For a complete list, see page 116.

Three graduate students in physics at Colorado University in Boulder who carried out their research at the NIST Boulder Labs under the supervision of Manny Knill of ACMD received their Ph.D. degrees in 2013. **Michael Mullan**, who completed a thesis entitled *Quantum Algorithms for Atomic Clocks*, accepted a position with Northrup Grumman. Following his thesis work on *Randomized Benchmarking of Clifford Operators*, **Adam Meier** moved on to the Georgia Tech Research Institute. **Yanbao Zhang** has relocated to Waterloo's Institute for Quantum Computation following his work on *Analysis of Tests of Local Realism*.

Passings

Saul Gass, a consultant to NIST from 1976 to 2013—most recently a faculty appointee in ACMD—died of cancer on March 17, 2013 at the age of 87. A professor emeritus in the University of Maryland’s business school, he was an internationally respected expert in operations research (OR), a mathematics-based discipline that uses advanced analytical methods to help organizations make better decisions.

Gass began his career in operations research in the field’s early years, working in the Pentagon in the early 1950s for George Dantzig. Dantzig was the principal developer of the simplex algorithm for linear programming, which is the cornerstone of the optimization methods that are among the most important tools in operations research. In 1958, Gass published the first-ever textbook on linear programming, a book that is currently in its fifth edition.

Gass became one of the field’s leading practitioners, serving as president of the Operations Research Society of America, and working as a senior manager at IBM contributing to the space program’s Project Mercury. In the latter half of his career, he became a senior statesman for OR, writing and editing books chronicling the history of the field. “Everybody in the field of operations research knew Saul Gass,” said Ronald Boisvert, chief of ACMD.

“Saul was one of the very last remaining grand pioneers of the relatively new field of operations research,” says Christoph Witzgall, a NIST researcher in the field of operations research from 1973 to 2003. “Beyond Saul’s impressive technical achievements, his role as a mentor, communicator, promoter, and organizer par excellence will be sorely missed.”

“It was a real privilege for us to have such a pioneer in our midst,” says Boisvert. “His encyclopedic knowledge of operations research was a great asset. Often when we had a ‘new’ and exciting problem to work on, we discovered that Saul had already made fundamental contributions to solving the problem years before. His advice was always thoughtful and helpful.”

The thread that runs through Gass’ NIST work was his evaluation of the ability of mathematical models to correctly guide critical decisions, adds Boisvert.

Although Gass had utilized NIST’s prototype computers in the 1950s while carrying out Air Force-funded projects, he first became a consultant to NIST in 1976 in order to aid the Operations Research Division of the Center for Applied Mathematics. In the early 1980s, Gass was offered the position of chief of NIST’s Operations Research Division, but he decided to stick with his full-time position teaching at the University of Maryland.

His work at NIST included evaluating oil and gas supply models for the Department of Energy, helping the Federal Emergency Management Agency prepare for national emergencies such as earthquakes and wars, improving the accuracy of 3-D coordinate measurement machines, and studying how the structure of computer networks and power grids contributes to their reliability.

Up until fall 2012, Gass continued to work at NIST one day per week, and his advanced age didn’t seem to slow him down. “An article about him in a leading operations-research journal was entitled ‘High-Octane Gass.’ Anyone who interacted with him understood that ‘high-octane’ reference immediately. His energy and enthusiasm were boundless,” says Boisvert.

“He was also a kind and gentle man. He always took the time to say kind words to our support staff, and he was a favorite of theirs as a result. We will miss his sparkle and vitality.”

Gass’ hobbies included jogging (which he continued doing as recently as last year), gardening, and reading mystery novels.

He is survived by his wife Trudy, their two children, and a granddaughter.

[A version of this article, which was developed by NIST Public Affairs, originally appeared on the NIST internal website.]



Figure 1. Saul Gass

Frank W. J. Olver, a faculty appointee in ACMD, died on April 22, 2013 of complications following knee surgery. He was 88. Affiliated with NIST since 1961, Olver was a world-renowned applied mathematician and one of the most widely recognized contemporary scholars in the mathematical field of special functions, which are the bread-and-butter tools for creating mathematical models in all areas of science. He was working at NIST two days a week up until February 2013.

Born in Croydon, England, Olver joined NIST's staff as a mathematician, coming from the UK's National Physical Laboratory (NPL), where he had been a founding member of the Mathematics Division and head of the Numerical Methods Section. NIST's Milton Abramowitz recruited Olver to be the author of the chapter "Bessel Functions of Integer Order" in the *Handbook of Mathematical Functions* (M. Abramowitz and I. Stegun, eds., 1964), a publication which went on to become the most widely distributed and most highly cited publication in NIST's history.

Olver is particularly known for his extensive work in the study of the asymptotic solution of differential equations, i.e., the behavior of solutions as the independent variable (or some parameter) tends to infinity, and in the study of the particular solutions of differential equations known as special functions (e.g., Bessel functions, hypergeometric functions, exponential integrals). His book *Asymptotics and Special Functions* (Academic Press, 1974) has become a classic. Having witnessed the birth of the computer age firsthand (as a colleague of the "father of computer science," Alan Turing, at NPL, for example), Olver is also well known for his contributions to the development and analysis of numerical methods for computing special functions.

In 2000, a 1,074-page commemorative volume *Selected Papers of F.W.J. Olver* was published by World Scientific Publishing Co. More than half of the 56 reprinted papers in the volume cite a NIST affiliation. In a review of that volume, Drexel University Professor Emeritus Jet Wimp said that the papers "exemplify a redoubtable mathematical talent, the work of a man who has done more than almost anyone else in the 20th century to bestow on the discipline of applied mathematics the elegance and rigor that its earliest practitioners, such as Gauss and Laplace, would have wished for it."

After leaving NIST's staff in 1986, Olver became a professor in the University of Maryland's mathematics department and in that university's Institute for Physical Science and Technology. However, he continued to maintain a connection to NIST. Most notably, he served as the editor-in-chief and mathematics editor of the online *NIST Digital Library of Mathematical Functions* (<http://dlmf.nist.gov>) and its 966-page print companion, the *NIST Handbook of Mathematical Functions* (Cambridge University Press, 2010). Fitting capstones to Olver's long career, these modern successors to the classic 1964 Abramowitz and Stegun handbook will extend its legacy well into the 21st century.

According to *Digital Library of Mathematical Functions* project lead Daniel Lozier, "Olver's encyclopedic knowledge of the field, his clear vision for mathematical exposition, his keen sense of the needs of practitioners, and his unfailing attention to detail were key to the success of that project." Olver himself was the author or coauthor of five of the 36 chapters. He continued editing work on the *Digital Library* until the time of his death.

In 2011 Olver was honored with the Department of Commerce Gold Medal and was inducted into the NIST Gallery of Distinguished Scientists, Engineers and Administrators. He was also a Fellow and charter member of the UK's Institute of Mathematics and Its Applications, as well as a foreign member of the Royal Swedish Academy of Sciences.

Among Frank's hobbies was the game of tennis. One of his favorite stories was about the time he hit the winning shot in a playoff match that catapulted NIST's team from the B league (lower division) into the A league (the best teams) of federal government inter-agency play for the first time ever.

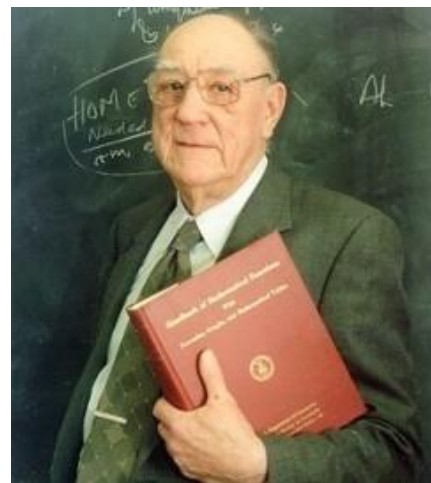


Figure 2. Frank W. J. Olver

Olver produced an impressive mathematical progeny. His son Peter is head of the School of Mathematics at the University of Minnesota. And Peter's son, Sheehan, is a lecturer in the School of Mathematics at the University of Sydney, Australia. Sheehan, a rising star in the field of numerical analysis, spent a summer as a NIST SURF student working on the *Digital Library of Mathematical Functions* project. Frank is also survived by his wife Claire, and daughter Sally Sondergaard.

[A version of this article originally appeared on the NIST internal website.]

Recognition

Division staff garnered a number of professional recognitions during the past year. These are described below.

ACMD staff members and associates were honored in four of the six annual ITL awards presented in 2013. **Stephen Jordan** received the Outstanding Journal Paper Award for his paper with Keith Lee and John Preskill entitled "Quantum Algorithms for Quantum Field Theories," which appeared in *Science* on June 1, 2012. Raghu Kacker was cited, along with colleagues from the ITL Information Access Division, with the Outstanding Conference Paper Awards for "Data Dependency on Measurement Uncertainties in Speaker Recognition Evaluation," published in the Proceedings of the 2012 SPIE Defense Security Sensing Conference. **Andrew Dienstfrey** and **Ronald Boisvert** received the Outstanding Contribution to ITL award for "pioneering efforts in the development and effective dissemination of research results and modern methodology advances in uncertainty quantification for scientific computing. And finally, **Yu (Jeff) Lei**, ACMD Guest Researcher from the University of Texas at Arlington, was tapped as ITL Associate of the Year, for "outstanding contributions to the combinatorial testing for software and systems project."

Ronald Boisvert of ACMD completed an unprecedented three terms (9 years) as Co-Chair of the Publications Board of the Association for Computing Machinery (ACM) on June 30, 2013. With more than 100,000 members, ACM is the world's largest educational and scientific society in the computing field. Its publications include more than 40 research journals, 8 magazines, 26 newsletters, as well as more than 450 conference proceedings volumes each year. The Publications Board develops editorial policies and procedures for the organization and appoints and oversees all of the volunteer Editors-in-Chief for ACM publications. In recognition of his service, the ACM Council, the organization's governing body, passed the following resolution at its June 14, 2013 meeting: "Whereas Ron Boisvert is completing his service as co-Chair of the ACM Publications Board, after nine years of leading the Board with vision, judgment, discretion, and dedication; and Whereas ACM's publications program has been strengthened extensively through Ron's leadership, including extensive growth in journal publication and extensive improvements in the ACM Digital Library. Council expresses ACM's appreciation for Ron Boisvert's exemplary and selfless service."



Figure 3. Ron Boisvert receives a certificate of appreciation from ACM President Vint Cerf at a meeting of the ACM Council in San Francisco in June 2013.

Part II

Features



Approximating the Ising Partition Function

The Ising model is a classical model in statistical mechanics of magnetization. Historically, this model has played a significant role in physics; the discovery of phase transitions within the model served as one of the first pieces of evidence supporting atomism, the claim that changes on an atomic scale could lead to large, observable changes. Due to its subtleties, the Ising model continues to be studied intensely by mathematicians, computer scientists, and physicists alike. The Ising model is very difficult to solve computationally. In fact, many difficult problems in materials science, bioscience and computer science can be formulated as special instances of the Ising model.

The Ising model represents a magnet acted on by an external field. An estimate of the partition function yields estimates for many important physical and thermodynamic quantities of the magnet and it is the partition function that we strive to find. Unfortunately, it has been proved that finding the partition function is very hard except for a few very restricted special cases, and so approximation methods have been devised. These are still unsatisfactory because near certain critical temperatures, always where there is the most interest, the methods become extremely slow. We have designed a radically new method based on combinatorics and graph theory that physicists can use in practice. It combines a heuristic sampling method with graph theoretic and linear algebraic ideas to give a method that is independent of temperature.

Isabel Beichl

The Ising model is a classical model in statistical mechanics of magnetization. Historically, it has played a significant role in physics; the discovery of phase transitions within the model served as one of the first pieces of evidence in support of atomism, the claim that small changes on an atomic scale could lead to large, observable changes. Due to its subtle complexities, the Ising model continues to be studied intensely by mathematicians, computer scientists, and physicists alike. In addition, the Ising model is a hard problem that is typical of many problems arising in materials science and bioscience. Other NP-hard problems can be formulated as instances of the Ising model [1].

The Ising model represents a magnet acted on by an external field. The magnet is represented by a graph $G = (V, E)$, where the vertices V are the atoms in the magnet. The graph is accompanied by an assignment σ of $\{\pm 1\}$ spins to each vertex, called a spin configuration, which represents the possible states of the atoms in the magnet. Each spin configuration appears in the model with a certain probability, which is governed by

the temperature, the strength and direction of the external field, and the correlation of the spins between neighboring atoms. Given values for these parameters, the (Boltzmann) probability distribution on the $2^{|V|}$ spin configurations is defined as: $\pi(\sigma) = f(\sigma)/Z$. The denominator Z , which is the sum of the $f(\sigma)$ over all spin configurations, is called the partition function. Since an estimate of the partition function yields estimates for many important physical and thermodynamic quantities of the magnet, it is this function that we strive to find.

Unfortunately, finding Z is hard. Except for a few very-restricted special cases, the problem of determining Z exactly is #P-complete. Therefore, we desire to find approximation algorithms for Z that run quickly. Currently, physicists use Markov chain methods that originated with the famous the Metropolis algorithm [5]. Although great improvements have been made to the basic Metropolis idea, all methods currently in use are known to be inefficient at low temperatures, and in fact, are not polynomial time algorithms. There is a Markov chain method of Jerrum and Sinclair [3], which they prove finds Z in polynomial time, but the order of the polynomial is large and so this algorithm is again too slow to use in practice.

Our aim has been to design an algorithm that physicists can use in practice. The algorithm that we created does just that. It combines a heuristic sampling method of Chen [2] (which generalizes the pioneering work of Knuth [4]) with graph-theoretic and linear-algebraic tools. This is a novel method that is not based on the Metropolis method, and which has not been previously investigated by the physics community. It brings the idea of Jerrum and Sinclair from complexity theory closer to the world of practical computation. We obtained a new insight into why computing near the critical point is slow and hard to do. It's not the temperature all by itself, it's the properties of the graph and how those properties are manifested when Z is evaluated near the critical temperature.

For fixed bond strength, computing Z is equivalent to counting the number of particular subgraphs of a graph G . Using the high temperature expansion, we can write Z and its derivatives as polynomials whose coefficients $c_{k,e}$ are the number of subsets of G with $2k$ vertices of odd degree and e edges. It is these coefficients that we estimate. In the absence of an applied field, a special case of interest, the problem of estimating Z reduces to estimating $c_{0,e}$. It is simple to restrict our method to the case of no odd degree vertices, which significantly reduces the complexity.

Counting these subgraphs is equivalent to counting the leaves of a particular search tree. We count these leaves approximately using Chen's stratified sampling. We construct a set of paths through the tree that identi-

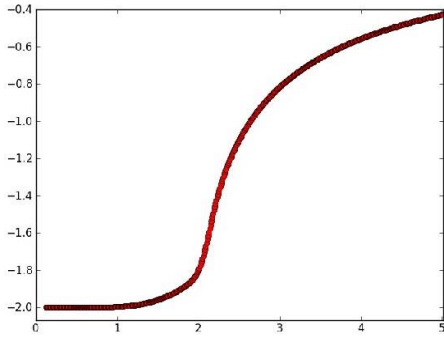


Figure 4. Estimate of mean energy 50,000,000 samples on a 16×16 grid as a function of $1/\beta = kT$.

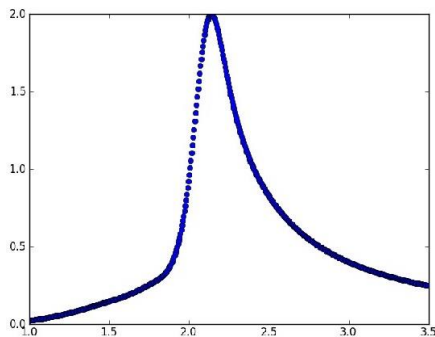


Figure 5. Estimate of specific heat using 50,000,000 samples on a 16×16 grid as a function of $1/\beta = kT$.

fies a stratum on each of the nodes, and agglomerates nodes in the same stratum together with one representative of the stratum selected at random. This greatly reduces the tree size but still gives a leaf sampling with more information than a single path.

The tree itself is formed from subgraphs of G , the nodes of the tree being the subgraphs. The symmetric difference of two subgraphs X_1 and X_2 written $X_1 \oplus X_2$, is the subgraph of G that contains precisely those edges in exactly one of X_1 and X_2 . One may consider this operation as addition of subgraphs over the field $\mathbb{F}_2 = \{0,1\}$. Let \mathcal{E}_0 be the set of *even subgraphs*, those subgraphs with no vertices of odd degree. Since the symmetric difference of two even subgraphs is again an even subgraph, we may view \mathcal{E}_0 as a vector space over \mathbb{F}_2 , called the *cycle space* of G . The dimension of the cycle space is $m - n + 1$, where m is the number of edges and n is the number of vertices. Hence, every set of $m-n+1$ linearly independent even subgraphs forms a *cycle basis* \mathcal{C} of G . Further, every even subgraph has a *unique* representation using the elements of \mathcal{C} , and $|\mathcal{E}_0| = 2^{m-n+1}$. The symmetric difference of a graph with $2k$ odd vertices and an element of the cycle basis (which has 0 odd vertices) is still a graph with $2k$ odd vertices.

We generate a cycle basis for G which can be done in polynomial time and construct the desired search

tree by starting with a subgraph with the desired $2k$ odd vertices and at each level of the tree we take the symmetric difference with one of the basis cycles of \mathcal{E}_0 , one cycle for each level. We estimate the number of vertices of this tree using the variation of Chen's stratified sampling method described above, without constructing the entire tree.

One of the problems with existing work on this problem is that near a critical temperature, the convergence become slower and slower. This new method is radically different in that it is temperature independent. A single run gets the partition function for all temperatures. The result is a fast and powerful code.

We have used this code to compute the coefficients of the partition function for the 2D and 3D Ising model. We generate the 2D and 3D phase transition. We also discovered a binomial approximation with great savings in computational cost. Three papers were written [6, 7, 8]. In Figure 4 and Figure 5, we show estimates of mean energy and specific heat after 50 000 000 samples of our algorithm on a 16×16 grid as a function of β^{-1} . We are also able to estimate mean magnetic moment and magnetic susceptibility.

References

- [1] A. Lucas, Ising Formulations of Many NP Problems, arXiv:1302.5843.
- [2] P. Chen, Heuristic Sampling: a Method for Predicting the Performance of Tree Searching Programs, *SIAM Journal on Computing* **21** (1992), 295–315.
- [3] M. Jerrum and A. Sinclair, Polynomial-time Approximation Algorithms for the Ising Model, *SIAM Journal on Computing* **22:5** (1993), 1087–1116.
- [4] D. E. Knuth, Estimating the Efficiency of Backtrack Programs, in *Selected Papers on Analysis of Algorithms*, CSLI Publications, Stanford, CA, 2000.
- [5] N. Metropolis, A. W. Rosenbluth, M. N. Rosenbluth, A. H. Teller and E. Teller, Equations of State Calculations by Fast Computing Machines, *Journal of Chemical Physics* **21:6** (1953), 1087–1092.
- [6] A. Streib, N. Streib, I. Beichl and F. Sullivan, Stratified Sampling for the Ising Model, in review.
- [7] A. Streib, N. Streib, I. Beichl and F. Sullivan, A Binomial Approximation Method for the Ising Model, in review.
- [8] A. Streib and N. Streib, Cycle Basis Markov Chains for the Ising Model, in review.

Participants

Isabel Beichl, Amanda Streib, Noah Streib (NIST); Francis Sullivan (IDA Center for Computing Sciences).

Compensating Operators and Stable Time Marching in Ill-Posed Nonlinear Evolution Equations

Reconstructing the past behavior of physical systems is of great interest in several environmental and geophysical contexts, such as pollution source identification [1, 2]. In many cases, such systems are governed by coupled nonlinear hyperbolic-parabolic partial differential equations. The most desirable computational approach in such problems would seek the use of explicit time differencing to march backward in time from the known current state of the physical system. However, due to ill-posedness in time-reversed parabolic equations, such step by step backward in time marching would necessarily be unconditionally unstable and lead to explosive noise amplification. We have developed a novel stabilized time-marching procedure for computing nonlinear parabolic equations on 2D rectangular regions, backward in time. Very little is known either analytically, or computationally, about this class of exponentially ill-posed problems. To quench the instability, the procedure uses easily synthesized FFT-based compensating operators at every time step. A fictitious nonlinear image deblurring problem is used to evaluate the effectiveness of this computational approach. The method is compared with a previously introduced, global-in-time nonlinear Van Cittert iterative procedure. The latter is significantly more time consuming, and impractical on large problems.

Alfred Carasso

Little is known, either theoretically or computationally, about backward in time continuation in multidimensional nonlinear parabolic equations. Various examples discussed in [3-6] highlight the fact that only limited success is generally possible in such problems. This is a consequence of the Hölder-continuous stability inequalities that characterize ill-posed continuation [7]. Nevertheless, two novel and significant computational approaches are developed in [4] and [5] that open new doors for further fruitful exploration. The method in [4] is a global in time iterative procedure originally designed for solving linear convolution integral equations. The approach in [5] is a backward time marching scheme where compensating operators are applied at each time step to quench the instability.

2D Nonlinear Parabolic Equations in Rectangular Regions. The work in [4] and [5] deals with a class of nonlinear parabolic equations on the unit square $\Omega \equiv \{0 < x, y < 1\}$ in the (x, y) plane, with homogeneous Neu-

mann boundary conditions on $\partial\Omega$. With fixed $T > 0$, the following initial value problem is a typical example

$$(1) \quad \begin{aligned} w_t &= \gamma r(w) \nabla \cdot \{q(x, y, t) \nabla w\} \\ &+ a\sqrt{|w|} w_x + b(w \cos^2 w) w_y \quad \Omega \times (0, T) \\ w(x, y, 0) &= g(x, y), \end{aligned}$$

where $\gamma = 0.04$, $a = b = 0.5$, $r(w) = \exp\{\cos^2(w)\}$, and $q(x, y, t)$ is given by

$$(2) \quad \begin{aligned} q(x, y, t) &= e^{10x}(1 + 5e^{2y} \sin \pi x) \\ &\geq 1 \quad \Omega \times (0, T). \end{aligned}$$

Instructive backward reconstruction experiments in such nonlinear equations result from the use of initial data $g(x, y)$ in the form of sharp 8-bit gray scale $IM \times IM$ pixel images, with pixel values ranging between 0 and 255. An explicit finite difference scheme is used to march the solution NT time steps Δt forward in time, up to time $T = NT \Delta t$. This results in a blurred version of the original sharp image. Reconstructing the initial data $g(x, y)$ from these computed data at $T = NT \Delta t$ represents nonlinear image deblurring. A significant advantage of such experiments is that visual recognition provides immediate evaluation of the extent of useful recovery using the different computational approaches.

Given the fixed finite difference mesh parameters $\Delta t = T/NT$, $\Delta x = \Delta y = 1.0/IM$, denote by Λ^T the forward in time nonlinear finite difference solution operator that transforms the initial image data $w(x, y, 0) = g(x, y)$ into the blurred image at time T , $w(x, y, T) = f(x, y)$, through the above explicit scheme computation.

Thus

$$\Lambda^T w(x, y, 0) = w(x, y, T)$$

i.e.,

$$\Lambda^T g(x, y) = f(x, y).$$

The following iterative approach has been found useful in many examples similar to Eq. (1).

Nonlinear Van Cittert Iterative Procedure. Given the blurred image data $f(x, y)$ at time T , fix λ such that $0 < \lambda < 1$. Let $h^1(x, y) = \lambda f(x, y)$, and consider

$$\begin{aligned} h^{m+1}(x, y) &= h^m(x, y) + \lambda\{f(x, y) - \Lambda^T h^m(x, y)\} \\ &\geq 1. \end{aligned}$$

Note that this involves repeated numerical solution of Eq. (1) using successive updated initial data $h^m(x, y)$. While this iteration cannot converge, good reconstructions can often be obtained by terminating this process after a finite number of iterations.

USEFUL DEBLURRING OF 512x512 NONLINEARLY BLURRED IMAGERY

Blur with anisotropic nonlinear parabolic equation (3 min).

Deblur with stabilized backward in time marching (4 min).

Deblur with 100 Van Cittert iterations (5 hrs).



Figure 6. In 512x512 resolution chart image, stabilized backward time-marching with $\varepsilon = 3.5 \times 10^{-4}$, $p = 2.5$, competently recovers vertical sequence of numbers near image right edge in relatively little computing time, while the Van Cittert iteration is computationally impractical on large problems.

Compensated Backward Time Marching in Eq. (1).

Let B denote the linear operator $-\Delta^p$, where p is any real number with $2 < p < 3$. In the present case of 2D problems in rectangular regions, the operator B can easily be synthesized using FFT algorithms. For problems in more general domains, the action $-\Delta^p$ can be synthesized from knowledge of a sufficient number of eigenpairs of the Laplacian on that domain. Such eigenpairs can be acquired *a priori*. With small $\varepsilon > 0$, one can stabilize backward time marching in the explicit finite difference scheme for Eq. (1), by applying the compensating operator $\exp\{-\varepsilon |\Delta t| B\}$ to the finite difference calculation after each time step. Here, the pair (ε, p) must be chosen interactively. However, there are infinitely many such useful pairs, and a good choice can generally be found after very few trials.

The present compensated marching approach differs from the *quasi-reversibility* method discussed in [7]. The latter method is restricted to linear parabolic problems

$$w_t + A(t)w = 0$$

and it uses the modified equation

$$w_t + A(t)w - \varepsilon A^*(t)A(t)w = 0$$

for backward continuation, where A^* is the adjoint of the elliptic differential operator A . However, an adjoint operator is not easily defined in the nonlinear case.

Two Examples. Figure 6 is a 512x512 US Air Force Resolution image. Nonlinear blurring was achieved by using an explicit scheme in Eq. (1) with $\Delta x = \Delta y = 1/512$, $\Delta t = 1.5 \times 10^{-7}$, and 600 time steps, to yield the blurred image at the final time $T = 9.0 \times 10^{-5}$. This blurring computation was accomplished in 3 minutes on a

modest personal workstation. Due to the pronounced anisotropic character of $q(x,y,t)$ in Eq. (2), the vertical sequence of numbers near the right edge has almost been erased. However, after 100 Van Cittert iterations in the rightmost image in Figure 6, that vertical sequence is partially restored, along with noticeable improvements in other parts of the image. As may be expected, that Van Cittert reconstruction required almost 5 hours, as it necessitated 100 successive nonlinear blurring computations, each lasting 3 minutes.

However, using $\varepsilon = 3.5 \times 10^{-4}$ and $p = 2.5$ in the compensated backward explicit scheme produced the middle image in Figure 6. The vertical sequence of numbers near the right edge appears better defined in the middle image than in the rightmost Van Cittert image. However, certain other parts of the image are marginally better recovered in the Van Cittert restoration. The above choice of (ε, p) was arrived at after several interactive trials, each lasting 4 minutes. Clearly, on a parallel computer, several such pairs (ε, p) can be explored simultaneously.

Figure 7 is a 256×256 satellite image. Here the blurring computation required 20 seconds, and very useful reconstruction is achieved after 100 Van Cittert iterations and 2000 seconds, as shown in the rightmost image in Figure 7. Again, interestingly, after a few 25 second interactive trials, equally good results can be achieved using the compensated backward explicit scheme with $\varepsilon = 6.5 \times 10^{-4}$ and $p = 2.35$.

Concluding Remarks. Only limited success is generally possible in solving nonlinear backward parabolic equations. In many cases, compensated marching schemes can produce useful reconstruction in large

USEFUL DEBLURRING OF 256x256 NONLINEARLY BLURRED IMAGERY

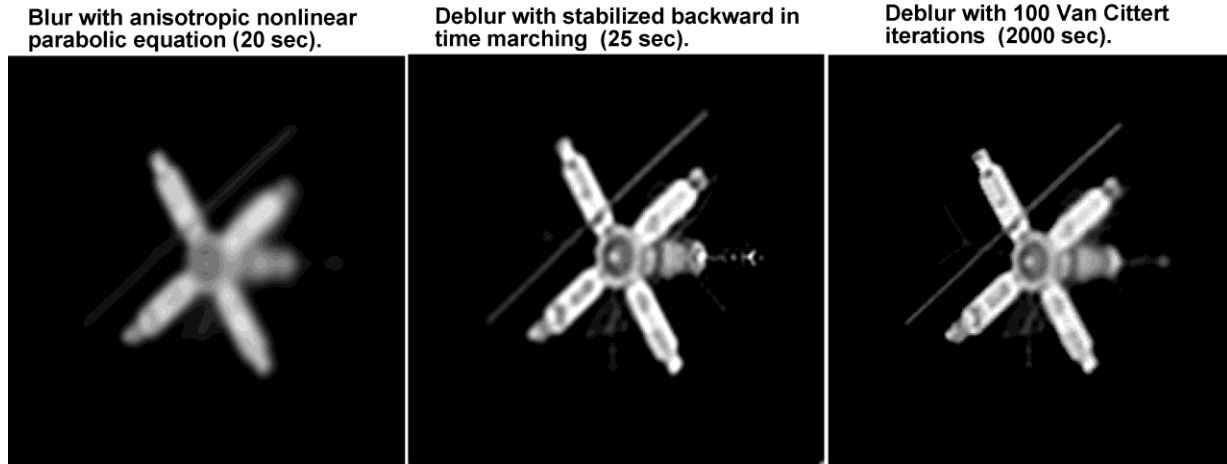


Figure 7. Stabilized backward time-marching with $\varepsilon = 6.5 \times 10^{-4}$, $p = 2.35$, produces a reconstructed Satellite image comparable in visual quality to that resulting from the computationally intensive Van Cittert iteration.

sized problems for which a global in time iterative procedure is computationally impractical.

References

- [1] J. Atmadja and A. C. Bagtzoglou, Pollution Source Identification in Heterogeneous Porous Media, *Water Resources Research* **37** (2001), 2113-2125
- [2] C. Bagtzoglou and J. Atmadja, Mathematical Methods for Hydrologic Inversion: The Case of Pollution Source Identification, Chapter 5 in *Handbook of Environmental Chemistry*, (2005), 65-96.
- [3] A. S. Carasso, Reconstructing the Past from Imperfect Knowledge of the Present: Effective Non-uniqueness in Solving Parabolic Equations Backward in Time, *Mathematical Methods in the Applied Sciences* **6:3** (2012), 249-261.
- [4] A. S. Carasso, Hazardous Continuation Backward in Time in Nonlinear Parabolic Equations, and an Experiment in Deblurring Nonlinearly Blurred Imagery, *Journal of Research of the NIST* **118** (2013), 199-217.
- [5] A. S. Carasso, Compensating Operators and Stable Backward in Time Marching in Nonlinear Parabolic Equations, NIST Internal Report, NISTIR 7967, (November 2013).
- [6] A. S. Carasso, A Stable Marching Scheme for an Ill-posed Initial Value Problem, in *Improperly Posed Problems and their Numerical Treatment*, (G. Hammerlin and K. H. Hoffman, eds.), Birkhauser-Verlag, Boston, 1983.
- [7] R. J. Knops, Logarithmic Convexity and Other Techniques Applied to Problems in Continuum Mechanics, in Symposium on Non-Well-Posed Problems and Logarithmic Convexity, (R. J. Knops, ed.), *Lecture Notes in Mathematics* **316**, Springer-Verlag, New York, 1973.
- [8] R. Lattes and J. L. Lions, *The Method of Quasi-Reversibility*, American Elsevier, New York, 1969.

Participants

Alfred Carasso

Single Photon Conversion Technology: Research to Commercialization

In a properly designed nonlinear optical device, single photons can be converted from one wavelength to another with near 100% efficiency. This technology has found numerous applications because of its ability to manipulate the frequency (that is, color) of nonclassical light while preserving its quantum properties. In the past few years, we have adapted this technology to develop highly efficient and sensitive single photon detectors for use in quantum communications. In addition, we have performed significant studies to optimize their use for advanced measurement science.

Continuing these developments, in FY 2013 the team proposed and demonstrated another technique called frequency-correlated bi-photon spectroscopy, which is potentially very important in cases where the spectral measurement can only be performed locally while the object is far away or somehow inaccessible. Additionally, the team jointly developed a more practical dual-channel single-photon up-conversion detector in collaboration with a team of Stanford University researchers. In such a dual-channel device, two detectors may be used at the same time so that the overall achievable data rate is doubled, which is advantageous in advanced communication systems.

Some of the techniques proposed by our team are being transferred to US industry via the NIST Small Business Innovative Research (SBIR) program. DARPA has also seen great promise for this technology; their most recent SBIR solicitation cited three publications from our team. Furthermore, high-efficiency frequency conversion is one of the building blocks needed for the development of quantum repeaters, which are necessary to move quantum-based cryptographic key exchange beyond point-to-point communications.

Xiao Tang

Light consists of a huge number of individual photons, each with a unique color. Single photon conversion technology can change the color, or in technical terms change the frequency, of a single photon of light using nonlinear optics. In a nonlinear optical device, two photons at lower frequencies can be combined into one photon of a higher frequency in a process called frequency up-conversion. Alternatively, a single photon at a high frequency can be converted to a pair of photons at lower frequencies, which is called frequency down-conversion. The quantum properties of the initial photon are preserved in the conversion process. This technology, known as "quantum frequency conversion"

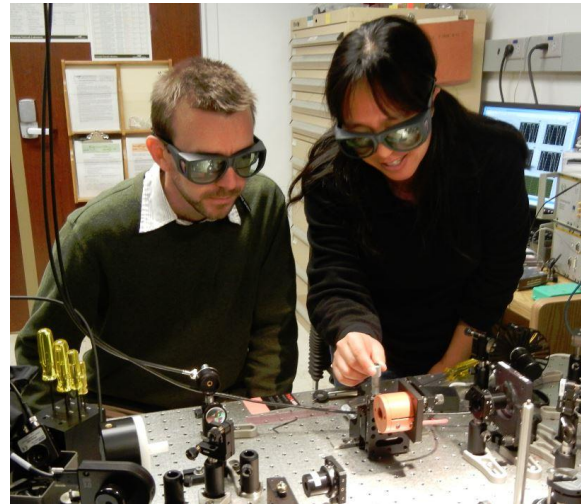


Figure 8. Paulina Kuo (right) and Oliver Slattery of ACMD work on a single photon conversion device.

(QFC), has found numerous applications because of its ability to manipulate the frequency of nonclassical light. For example, advanced optical communications applications, including single-photon quantum communications and quantum information processing for provably secure data links, can benefit from operating in both the visible and the near-infrared (NIR) wavelengths. In principle, QFC provides a way to coherently convert between visible photons (best for photon processing, storage, and detection) and NIR photons (best for long-haul transmission through fiber at commercial telecommunication bands).

Previous work. By using the up-conversion technique, near-infrared light can be converted to light in the visible or near visible range where it can be detected by low-cost commercially available detectors with low-noise and high efficiency. In recent years, ITL's quantum communication research team has developed up-conversion single photon detectors in the NIR range by using long-wavelength pump light. These detectors were used in NIST quantum key distribution (QKD) systems at an operating wavelength of 1310 nm, significantly increasing the operating distance over existing systems while maintaining very high speed [1]; this work won an R&D 100 Award in 2007.

Due to conservation of energy, the frequency of the pump light varies, and only signal photons at the corresponding frequency can be converted and detected. In this way, the spectrum of the signal photon can be measured if we vary the wavelength of the pump light. In 2009 we developed an up-conversion spec-

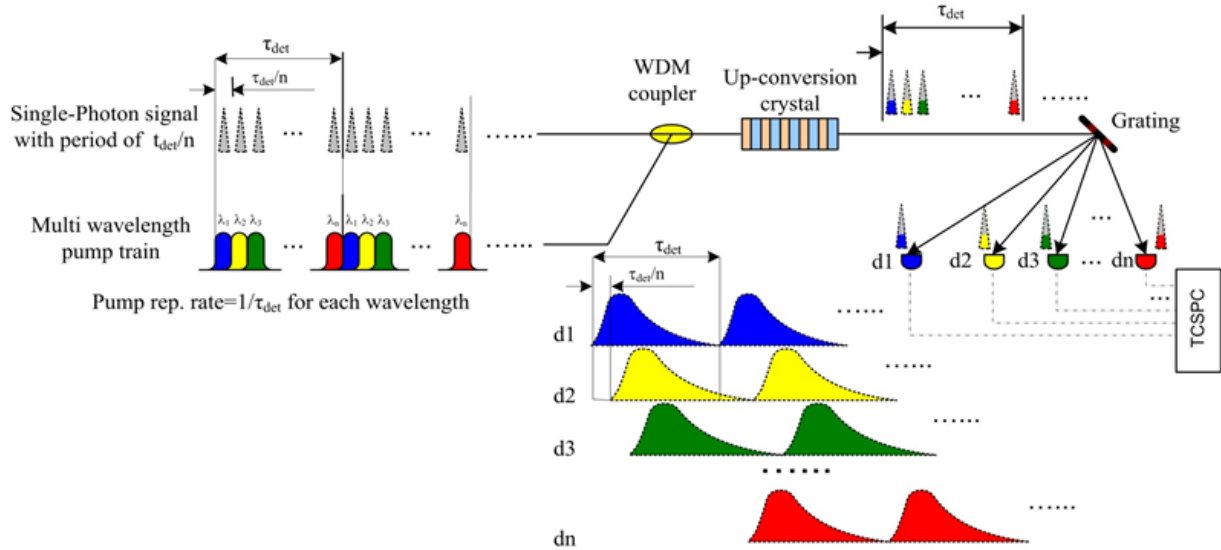


Figure 9. With the pump beams at different colors (wavelengths), the signal photon pulses are converted to different wavelengths. They can be separated by a grating and detected by detectors (one for each wavelength). The detected data can be restored at a multiplied rate, beyond the intrinsic data rate limitation.

trometer based on this principle [2], which can be used to measure the spectrum of extremely weak, single-photon-level optical signals. Its sensitivity is three orders of magnitude higher than any existing commercial spectral instrument.

Our team has used these single photon up-conversion detectors and spectrometer in a variety of research projects including

- implementation of a high-speed quantum key distribution system;
- demonstration of a detector with a temporal resolution better than the jitter-limited resolution of commercial single photon detectors;
- characterization of an entangled photon pair source, including a direct spectrum measurement for photons generated in spontaneous parametric down-conversion;
- characterization of single photons from quantum dots including the measurement of carrier lifetime with high accuracy, and the demonstration of preservation of non-classical features of the converted photons;
- observation of 2nd, 3rd and 4th order temporal correlations of near infrared single photons from coherent and pseudo-thermal sources following frequency up-conversion;
- study of the time-resolving measurement capability of up-conversion detectors using a short pulse pump; and
- evaluation of the modulation of a single photon wave packet for better interfacing of independent sources.

These efforts by the ITL quantum communication team were summarized in a comprehensive review article published in *Physics Reports* [3]. This article demonstrates that the team is a world leader in research and development in this field.

Recent Developments. In FY 2013 we have undertaken work to improve the performance of the devices, and to expand their application. Three such efforts: “Frequency Correlated Bi-Photon Spectroscopy,” “Dual-channel Single-photon Upconversion,” and “Two-photon Interference with Coherent Pulses” are described below. In addition, the team continues to work to transfer their technology to US industry for commercialization.

Frequency Correlated Bi-Photon Spectroscopy. Our demonstration of frequency correlated bi-photon spectroscopy is based on combining the ITL up-conversion spectrometer and the ITL correlated photon pair source. The photon pair source generates correlated photon pairs using a frequency down-conversion technique; one photon of the pair is in the telecommunication band (~ 1310 nm, useful for long-haul transmission) and the other is in the near visible range (~ 895 nm, useful for storage in the Cesium atomic system). These correlated photons are similar to twins; they were born at same time and their characteristics are also correlated with each other. For example, once the wavelength (or frequency) of one photon is determined, the wavelength of the other is also known by energy conservation. The photons at one wavelength can be sent as a probe to interact with a remote or inaccessible object. In principle, the spectral func-

tion of the remote object can be determined by locally measuring the correlated ‘twin’ photon at another wavelength using an up-conversion detector and monitoring the coincidence of the twin photon pairs. The ITL quantum communication team proposed and demonstrated this technique. The results were published in *Laser Physics Letters* [4]. This technique is potentially very important in cases where the spectral measurement can only be performed locally while the object to be measured is far away or inaccessible.

Frequency correlated bi-photon spectroscopy provides a new way to measure spectral properties of remote objects. However its functionality and performance can be further improved. For example, it is important to have high spectral resolution in the spectrum measurement. In the current experimental configuration, the spectral resolution is determined by the spectral response function of the frequency conversion process in the device. In order to improve the spectral resolution, the ITL team carefully investigated the relationship of the spectral response function, pump condition, and other parameters in the device. In this way, optimized operating conditions can be predicted and achieved for better spectral resolution. A detailed analysis was published in *Optics Express* [5].

Dual-channel Single-photon Upconversion. The data transmission rate of a quantum communication system using silicon based single-photon detectors is limited by the jitter in the detectors. In FY 2010 the team proposed and experimentally demonstrated a multi-wavelength pumping technique that multiplied the data rate of such systems beyond their intrinsic jitter limitation [6]; see Figure 9. Based on this idea, the team recently developed a more practical dual-channel single-photon up-conversion detector in collaboration with Stanford University researchers [7]. In a regular single channel up-conversion detector, signal photons in the telecommunication band can be converted to a wavelength (λ_1) in the visible range by using a pump beam at another wavelength using the up-conversion technique. In the dual channel device, if two pump beams alternate at slightly different wavelengths, the signal photons can be converted to two slightly different wavelengths (λ_1, λ_2) in the visible range. These converted photons can in turn be separated by a dispersion element and then detected by two separate photon detectors. The data from the two detectors can then be combined into one data stream. In such a dual channel device, the data rate in each channel is still intrinsically limited by the jitter of the detector, but the combined data rate is doubled. This technology provides an important solution for the higher data rate requirements in advanced communication systems.

For further improvement in noise reduction, the team carefully investigated a variety of spectral filtering techniques with this dual channel up-conversion detector and found that volume Bragg gratings are the

best choice for up-conversion single photon detectors for simultaneously achieving low noise and high conversion efficiency [8].

Two-photon Interference with Coherent Pulses. Photon interference is one of the most fascinating topics in optical physics. Photon interference studies aim to understand the nature of the phenomenon, as well as its application in quantum information science. In FY 2013, the team observed photon interference with coherent pulses [12]. This is the first step in the preparation for the future development of a quantum repeater.

Technology Transfer. The team has also worked to enable the transfer of its technology to US industry to enable commercialization. In particular, US companies AdvR and Lepton Technology received funding from the NIST SBIR Program to develop technology based on the NIST up-conversion device described earlier [1]. Phase 1 and Phase 2 of this SBIR project were successfully completed in FY 2013. Soon after, another NIST SBIR project was initiated to enable US Company Gener8 to further develop the NIST technique of using a Bragg grating embedded on a non-linear single photon source for enhanced narrowband photon pair creation [9].

Additional development and commercialization of ITL’s technology is now being spearheaded by DARPA, who recently announced an SBIR solicitation [10] based mainly on the technology developed at NIST. Three articles by the ITL team [2, 6, 11] were cited in the solicitation.

Future Plans. One of the ITL team’s long-term goals is the development of quantum repeaters. Current quantum communication technology can only be done by point-to-point communication. The distance in which this can be done is limited by signal attenuation in the transmission medium, e.g., optical fiber or the atmosphere. In classical telecommunications, “repeaters” read an incoming digital signal, restore its fidelity and retransmit it to the next node along a path to its ultimate destination. Quantum repeaters have the same function, but they must operate in a different way. Due to the no-cloning rule of quantum mechanics, the incoming qubits cannot be directly read, lest their information content be lost. Instead, the incoming quantum state must be purified and enhanced to restore its fidelity and then passed to the next node without being directly read by using a sophisticated technique based on entanglement swapping. This is quite challenging; a quantum repeater is, in essence, a special purpose quantum computer.

The quantum frequency conversion described above is one of the building blocks needed for the development of quantum repeaters. The ITL team is working on other elements for this long-term goal as well. For example, the ITL team has started the effort

to design and implement entangled photon pair sources. This is part of a collaborative NIST Innovation in Measurement Science (IMS) project, entitled “Quantum Randomness as a Secure Resource”. In addition, the team recently initiated collaboration with Washington University to develop narrow-band entangled photon pair sources based on micro-toroids. Entangled photon pair sources are important building blocks, not only for quantum repeaters, but also for quantum randomness required for secure communications.

Another example is to further study photon interference phenomenon based on the observation of photon interference with coherent pulses [12]. The team recently started a project to observe photon interference from independent single photon sources.

Another critical device, called a quantum interface, has been designed and is in the process of implementation in the lab. It will convert photons in the telecom wavelength band to an atomic transition wavelength, while preserving their non-classical features. Such a capability would connect telecom photons (for transmission) with atomic quantum systems (for storage). Furthermore, the team initiated a quantum memory project, which is a core component of the quantum repeater. Each of these ambitious and challenging research tasks is a necessary building block that will see final integration into a future quantum repeater.

References

- [1] H. Xu, L. Ma, A. Mink, B. Hershman and X. Tang, 1310-nm Quantum Key Distribution System with Up-conversion Pump Wavelength at 1550 nm, *Optics Express* **15:12**, (2007), 7247.
- [2] L. Ma, O. Slattery and X. Tang, Experimental Study of High Sensitivity Infrared Spectrometer with Waveguide-based Up-conversion Detector, *Optics Express* **17:16** (2009), 14395.
- [3] L. Ma, O. Slattery and X. Tang, Single Photon Frequency Up-conversion and its Applications, *Physics Reports*, **521:2** (2012), 69-94.
- [4] O. Slattery, L. Ma, P. Kuo, Y.-S. Kim and X. Tang, Frequency Correlated Bi-Photon Spectroscopy using a Tunable Up-Conversion Detector, *Laser Physics Letters* **10** (2013), 075201.
- [5] P. S. Kuo, O. Slattery, Y.-S. Kim, J. S. Pelc, M. M. Fejer and X. Tang, Spectral Response of an Upconversion Detector and Spectrometer, *Optics Express* **21:19** (2013), 22523.
- [6] Lijun Ma, Joshua C. Bienfang, Oliver Slattery and Xiao Tang, Up-conversion Single-photon Detector using Multi-wavelength Sampling Techniques, *Optics Express* **19:6** (2011), 5470.
- [7] J. S. Pelc, Paulina S. Kuo, Oliver Slattery, Lijun Ma, Xiao Tang, and M. M. Fejer, Dual-channel, Single-photon Upconversion Detector at 1.3 μm , *Optics Express* **20:17** (August 2012), 19075.
- [8] P. S. Kuo, J. S. Pelc, O. Slattery, Y.-S. Kim, M. M. Fejer, and X. Tang, Reducing Noise in Single-photon Frequency Conversion, *Optics Letters* **38:8** (April 2013), 1310.
- [9] L. Yan, L. Ma, and X. Tang, Bragg-grating-enhanced Narrowband Spontaneous Parametric Downconversion, *Optics Express* **18:6** (March 2010), 5957.
- [10] See DARPA SBIR solicitation SB133-001, Title: Efficient quantum frequency conversion for advanced optical communications⁷.
- [11] J. S. Pelc, C. R. Phillips, Q. Zhang, C. Langrock, O. Slattery, X. Tang, M. M. Fejer, Long-wavelength-Pumped Upconversion Single-photon Detector at 1550 nm: Performance and Noise Analysis, *Optics Express* **19** (2011), 21445.
- [12] Y.-S. Kim, O. Slattery, P. S. Kuo, and X. Tang, Conditions for Two-photon Interference with Coherent Pulses, *Physical Review A* **87** (2013), 063843.

Participants

Xiao Tang, Paulina Kuo, Lijun Ma, Oliver Slattery, Yong-Su Kim, Alan Mink and Barry Hershman (ACMD); Joshua Bienfang (NIST PML); Martin Fejer and Jason Pelc (Stanford University); Li Yan (University of Maryland Baltimore County)

⁷ <http://www.acq.osd.mil/osbp/sbir/solicitations/sbir20133/darpa133.htm>

Analysis for Dynamic Metrology

Diverse measurement contexts require estimates of time-varying quantities. Ideally the measurement device responds to signal variations significantly more rapidly than the modulation of the underlying signal. If so, then well-developed techniques may be used for the calibration and analysis of the measurement system. By contrast, as the characteristic timescales for signal modulation and measurement response become commensurate, the situation becomes more complicated; directly measured quantities may require correction for the finite bandwidth of the measurement system response. Toward this goal heuristic estimation rules have evolved over time and are now widely used. We rederive one common rule of thumb, and present sufficient conditions for its validity. Furthermore, we investigate its quantitative performance in cases for which these conditions are violated and encounter surprisingly poor results. While our work is directly relevant to high-speed communication systems, the fact that the analysis structures are universal to any linear, time-invariant system may serve as a cautionary tale for new research initiatives focusing on dynamic metrology ongoing at counterpart metrology institutes.

Andrew Dienstfrey

In collaboration with NIST PML, we are providing precision calibration and measurement services for waveforms as required by high-speed data systems. Figure 10 provides a representative example of the problem. The figure shows an eye-diagram, a standard diagnostic for digital waveform generators. The procedure superimposes a random bit stream such that all possible binary transitions appear. A mask region defines a pass/fail test for the generator as a signal falling within this region confounds the determination of the bit: 0 or 1. In Figure 10, the generator on the left passes the test while the generator on the right fails. The issue here is that these eye diagrams represent the same generator; the difference is in the oscilloscope used to measure the signal! Which measurement is correct? Private communications with industry representatives indicate that measurement ambiguity results in significant overhead costs.

The source of the problem lies with the dynamic response characteristics of the oscilloscope relative to the underlying signal. High-speed pattern generators are designed to deliver binary transitions on the order of 10 picoseconds (ps) or less, yet the fastest oscilloscopes available have impulse response functions with full-width-half-max times of 4 ps to 7 ps, only marginally faster. For situations requiring high accuracy, the measurement system cannot be considered ideal and

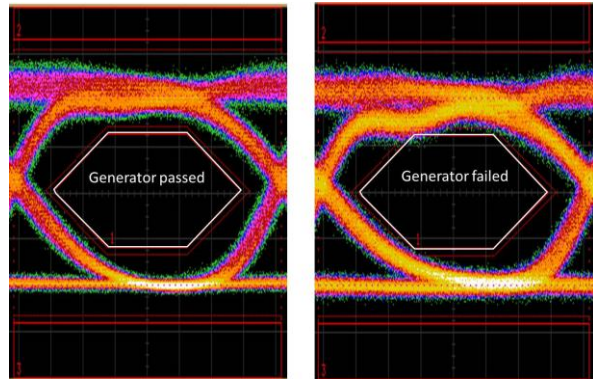


Figure 10. The “eye-diagram” diagnostic for a digital signal generator depends on the dynamic response of the measurement. The generator on the left passes the test while the generator on the right fails. The problem is that this test applies to the same generator as measured by two different oscilloscopes!

the directly measured signal must be corrected for finite bandwidth effects.

Unfortunately, implementing these corrections correctly incurs significant costs in the form of increased measurement and analysis requirements. Rules of thumb have been developed over time as shorthand to avoid this penalty. In the following we present an elementary derivation of one of these heuristics, and demonstrate that it rests on shaky ground as a quantitative tool. Even more, the foundational assumptions about the qualitative nature of the correction turn out to be unfounded. Details can be found in [1] and [2].

Waveforms Parameters and Analysis. We assume that the measurement can be modeled as a linear, time-invariant system in which case its analysis is cast as a convolutional equation,

$$y(t) = \int_{-\infty}^{\infty} a(s)x(t-s) ds. \quad (1)$$

Here $a(t)$ is the system response function, $x(t)$ the noise-free input waveform, and $y(t)$ is the noise-free output. Estimation of any one of these functions in a noisy measurement context arises as a canonical problem. For convenience, here we restrict attention to the scenario in which $x(t)$ is an impulse waveform. A practical example of this could be using a high-speed oscilloscope to measure the impulse response function of a photodiode used to convert optical signals to electrical. Measurement of digital waveforms proceeds analogously once technical difficulties are resolved related to the lack of a Fourier transform.

Given a time-varying waveform, $x(t)$, different metrics are used to quantify its speed of variation. The speed of an impulse response function is routinely quantified by its full duration at half maximum, denoted by $\tau_F(x)$. For step-like waveforms this role is played

by the transition durations between states, usually 10% to 90% denoted by τ_R . In addition to τ_F , an alternative definition of response has been proposed:

$$A = \int x(t) dt \neq 0 \quad (2a)$$

$$\mu(x) = \frac{1}{A} \int t x(t) dt \quad (2b)$$

$$\tau_\sigma^2(x) = \frac{1}{A} \int (t - \mu)^2 x(t) dt \quad (2c)$$

Of course Eq. 2 assumes that the moments exist and that the total integral is not zero; this can be verified for the impulse-response functions relevant to our work. The final equation Eq. 2c defines an alternative characterization of the speed of an impulse-like waveform that while not in wide use, has been advocated in some contexts. More importantly Eq. 2 plays a central role in motivating the next idea.

Returning to our measurement problem, a detailed analysis involves: (1) obtaining an estimate of $a(t)$, for example by a separate calibration experiment; (2) making a measurement of $y(t)$; and (3), inversion of Eq. 1 for $x(t)$. In addition to the substantial measurement burden required to characterize time-dependent functions, the final step is complicated and delicate as deconvolution is generically an ill-posed problem requiring regularization to stabilize the inversion in the presence of noise.

Across the wide-ranging landscape of heuristic analyses developed as an alternative, the most common conventional wisdom is that the finite bandwidth of the

measurement system results in a measured waveform that is *slower* than the true signal. If nothing else, it follows that the speed of $x(t)$ should be corrected for this effect. The formula that is nearly universally used to estimate this correction is

$$\tau_F(x) \approx \sqrt{\tau_F(y)^2 - \tau_F(a)^2} \quad (3)$$

We will refer to this approximate correction as root-sum-of-squares or RSS. The advantages of RSS over the convolutional analysis are obvious but bear repeating. For one, RSS only requires estimates of a single parameter representing waveform speeds, in place of the complete characterization of all waveforms as a function of time. Furthermore, in contrast to the issue of regularization, RSS inversion is easy to implement and analyze.

Despite the widespread use of RSS, we have been unable to find a derivation that includes clear conditions for its validity. Here we offer one. The definition of τ_σ is reminiscent of the definition of variance of a random variable. In this analogy the role of the probability density function is played by $x(t)$. While the scaling by $1/A$ normalizes the integral mass to be one, $x(t)$ generally oscillates and is not of one sign. Despite this, a simple computation shows that the analog to the additivity of variance law nevertheless follows. More precisely, assuming the measurement model, Eq. 1, and that the quantities in Eq. 2 exist, one may show that

$$\tau_\sigma^2(y) = \tau_\sigma^2(x) + \tau_\sigma(a)^2.$$

Thus we have the desired RSS relationship, only written with respect to the dubious quantities τ_σ as opposed to τ_F . Introducing a constant as the ratio between these two waveform parameters, $\tau_\sigma^2(x) = \tau_F(x)^2 k_F(x)$, we can state the following sufficient conditions for RSS.

Fact 1. *Given the convolutional relation Eq. 1, if $k_F(y) \approx k_F(x) \approx k_F(a)$, then $\tau_F(y)^2 \approx \tau_F(x)^2 + \tau_F(a)^2$.*

A similar constant, k_R , may be defined with respect to step waveforms, and likewise the constancy of this constant serves as a sufficient condition for an RSS formula involving τ_R .

Figure 11 shows the constants (k_F, k_R) for a variety of waveforms. The red x's show the values of the constants for three classical low-pass filters (Chebyshev, Butterworth, and Bessel-Thompson) of orders two through six. The blue

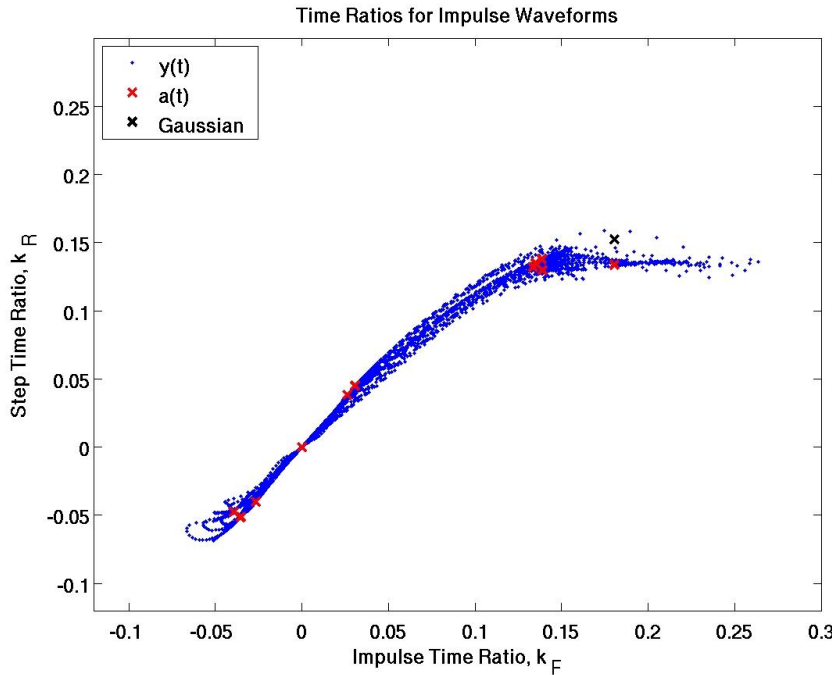


Figure 11. Values of the ratios (k_F, k_R) for elementary filters (red x's) and their pairwise convolutions (blue dots). The non-constancy of these ratios results in a corresponding violation of a simple RSS relationship for τ_F .

dots show all possible pairwise convolutions over a wide range of relative bandwidths. The first observation is that the time ratios (k_F , k_R) cannot be considered universal. It follows that the desired quantitative RSS relationship for τ_F is dubious. Even more striking is the fact that the ratios can be negative, suggesting that the finite bandwidth effects of measurement can result in a waveform that appears *faster* than the underlying input. Additional numerical experiments have confirmed this fact. In summary, not only does RSS fail to provide quantitative estimates of dynamic correction, the deeper and more foundational qualitative assumption that a measured waveform is slower than its input can also be erroneous.

Dynamic Metrology. For communications applications, the need to correct measurements for finite bandwidth effects has been understood for some time. One (perhaps simplistic) explanation is that the insatiable thirst for greater bandwidth results in the scenario that devices to generate, receive, and measure communications waveforms are based on nearly commensurate technologies. Increasingly, the dynamic paradigm is becoming relevant for measurements that heretofore were analyzed under static considerations. For example, in the automotive industry, precise, detailed measurements of the time-varying pressure inside combustion chambers are desired to improve fuel efficiency. Under normal operation, pressure can vary significantly over times on the order of tens of microseconds, yet until recently, SI⁸ traceable calibration of pressure sensors has been performed exclusively for static loads. In response, several European metrology institutes have embarked upon an extensive and coordinated re-evaluation of their measurement services for time-varying pressure, force, and torque [3, 4, 5].

Following [6], we define a *dynamic measurement* as one in which the measurand varies in time sufficiently fast relative to the response of the measurement system that corrections for finite bandwidth effects are required to achieve the desired accuracy. This definition makes clear that it is neither the absolute timescale nor physical application that is relevant for the designation. Rather, the common characteristics are the essential time-varying nature of the measurand, and the commensurability of the timescale of this variation relative to the response time of the measurement device. It follows that while the physical details of dynamic measurements may be very different, elements of the measurement analysis are shared. We expect that future collaborations across these application areas will serve to identify foundational concepts for the calibration and analysis of dynamic measurement systems.

References

- [1] A. Dienstfrey and P. D. Hale, Colored Noise and Regularization Parameter Selection for Waveform Metrology, *IEEE Transactions on Instrumentation and Measurement*, to appear.
- [2] A. Dienstfrey and P. D. Hale, Analysis for Dynamic Metrology, *Measurement Science and Technology*, to appear.
- [3] T. Bruns, Publishable JRP Summary Report for JRP IND09 (Dynamic) Traceable Dynamic Measurement of Mechanical Quantities, European Association of National Metrology Institutes (EURAMET), Technical Report JRP-IND09⁹, Nov. 2012.
- [4] T. Esward, C. Matthews, S. Downes, A. Knott, S. Eichstädt and C. Elster, Uncertainty Evaluation for Traceable Dynamic Measurement of Mechanical Quantities: A Case Study in Dynamic Pressure Calibration, in *Advanced Mathematical and Computational Tools in Metrology and Testing IX* (F. Pavese, M. Bär, J.-R. Filtz, A. B. Forbes, L. Pendrill, and K. Shirono, eds.), World Scientific Publishing Company, 2012, 143-150.
- [5] C. Bartoli, M. F. Beug, T. Bruns, C. Elster, T. Esward, L. Klaus, A. Knott, M. Kobusch, S. Saxholm and C. Schleger, Traceable Dynamic Measurement of Mechanical Quantities: Objectives and First Results of the European Project, *International Journal of Metrology and Quality Engineering* **3:3** (January 2012), 127-135.
- [6] T. J. Esward, C. Elster and P. Hessling, Analysis of Dynamic Measurements: New Challenges Require New Solutions, in *Proceedings of the XIX IMEKO World Congress*, Lisbon, Portugal, September 6-11, 2009, 2307-2310.

Participants

A. Dienstfrey (ACMD); Paul Hale (NIST PML)

⁸ International System of Units, <http://www.bipm.org/en/si/>

A Framework for Reproducible Latent Fingerprint Enhancements

Fingerprint evidence is routinely used to convict offenders of crimes, but such evidence is of highly variable quality, suffering from incompleteness, pressure gradations, and background variability. Due to the low signal quality of the fingerprint, these images are not suitable for input into fingerprint identification software. Because of this, the forensics community currently uses a variety of image processing tools to improve the quality of these images before attempting to identify a match. As dramatic and essential as these transformations are, no research exists to characterize this step of the evidentiary analysis chain. Fundamental questions about reproducibility, traceability, and quantification of accuracy remain. The aim of this work is to develop independent, systematic, and easily reproducible alternatives to forensic image preprocessing that can yield fingerprint enhancements of comparable quality. Such alternative approaches provide a valuable frame of reference that may be helpful in informing, complementing, and possibly validating existing methodology.

Alfred Carasso

In recent years, the reliability of fingerprint evidence has come under increased scrutiny, [1-5]. One area of concern involves the digital enhancement of latent fingerprints left unintentionally at a crime scene. Such prints are generally smudgy, with poorly defined ridge impressions that may be partially obscured by background structural detail, together with superimposed random noise. There may also be overlapping prints. A key step in obtaining latent print enhancements that has been stressed by numerous researchers involves isolating ridge impressions from such backgrounds. In a recent comprehensive NIST study [6, Chapter 4], the possibility of misleading artifacts in digital enhancements is discussed, with guidelines proposed for the proper evaluation and acceptance of enhanced images. These guidelines include validation of the enhancement technology, along with maintenance of an audit trail of the digital procedures used.

Photoshop¹⁰ processing is the preferred methodology among law enforcement forensic analysts for the enhancement of latent fingerprint images. Aiming to meet the requirements of automated fingerprint identi-

¹⁰ The commercial software products IDL, Matlab, Photoshop and PV-WAVE are identified in order to specify experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement NIST, nor is it intended to imply that the software identified are necessarily the best available for the purpose.

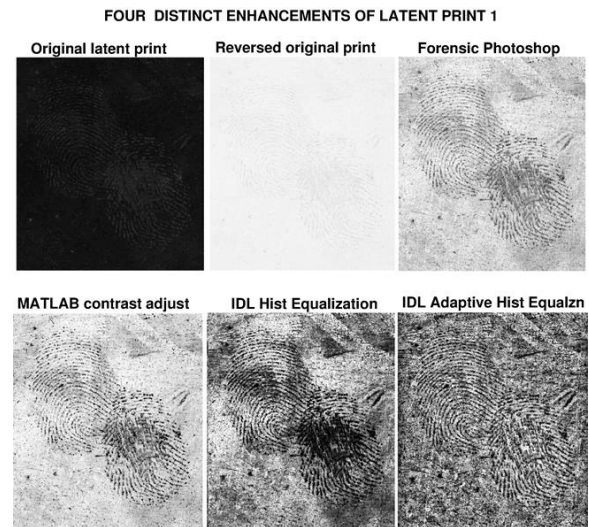


Figure 12. Four distinct enhancements of latent fingerprint 1. Possibly significant background structures are suppressed in Forensic Photoshop and MATLAB contrast adjusted images. IDL Histogram images produce better defined ridge impressions, along with considerable background information. Such background detail can be attenuated by reproducible fractional diffusion smoothing, as shown in the next figure.

fication systems (AFIS), forensic Photoshop enhancements typically strive to achieve an image exhibiting black ridge impressions over a quasi-uniform light grey background. A variety of “dodge and burn” and “brush” tools are typically applied to lighten or darken selected areas within the image, and remove unwanted background information. The multiplicity and diversity of the individual steps used in this process are not fully documented, and the procedure may not be reproducible. Viewing such enhancements without some frame of reference cannot allay the apprehension that potentially significant information may have been inadvertently eliminated, or artifacts possibly introduced, by overzealous application of image tools more appropriately used for retouching photographs, removing wrinkles, or darkening gray hair. These are some of the reasons why such fingerprint enhancements have occasionally been challenged.

Alternative Latent Fingerprint Enhancements. As shown in Figure 12, it is possible to achieve fully reproducible enhancements, comparable in visual quality to AFIS-ready forensic Photoshop enhancements, using scientific image analysis software tools that are independent of Photoshop. In [7] and [8], several alternative fingerprint enhancement approaches are discussed, along with the software routines necessary to implement them. All of these methods aim at bring-

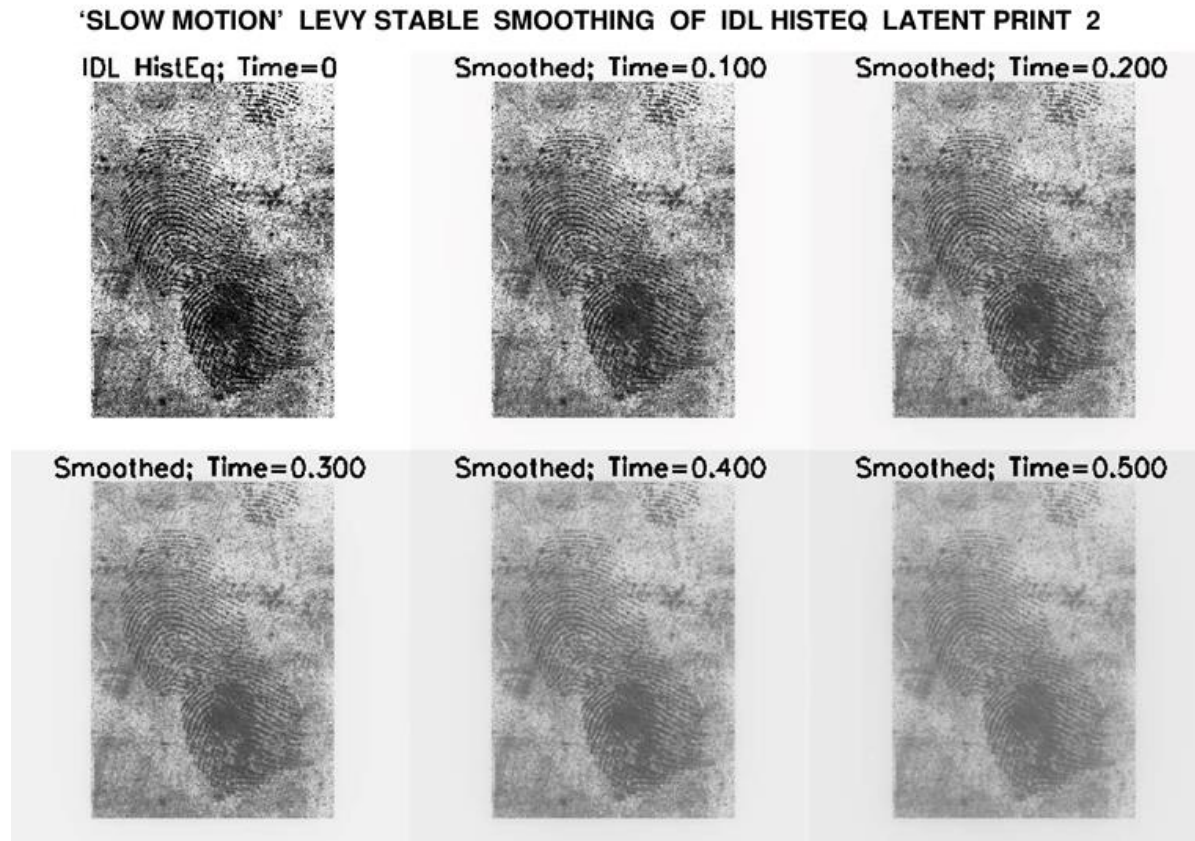


Figure 13. Progressive smoothing of IDL Histogram Equalized latent fingerprint 2, by solving Levy stable fractional diffusion equation from time $t=0$ to time $t=0.5$. Smoothed image at time $t=0.4$ appears to be optimal visually.

ing into better visual range potentially significant structures that are present in the image, but not easily discernible. Each of these enhancement methods is based on the use of a single command from such widely used scientific image analysis packages as MATLAB [9], IDL [10], and PV-WAVE [11]. Such enhancement commands are applied to the whole image at once, are executed in seconds, and are obviously reproducible. In addition, [12] provides a thorough discussion of the theory underlying these techniques.

Progressive Levy Smoothing of Histogram Equalized Latent Fingerprints. Of particular interest in latent print enhancement are the IDL commands that produce Histogram Equalization, and Adaptive Histogram Equalization, respectively. These two distinct IDL techniques generally exhibit better-defined ridge structure, along with considerably more background detail than is the case in forensic Photoshop enhancements. However, while some of this detail may be valuable contextual information in certain cases, there is also typically a great deal of noise and background clutter that can obscure useful ridge impressions. As shown in Figure 13, an effective smoothing technique, previously used successfully in nanoscale imaging [13], can be applied to gradually attenuate background detail while preserving ridge information.

The success of this smoothing technique hinges on two significant factors. First, the smoothing diffusion equation involves the Laplacian operator raised to a low fractional power, such as $p=0.2$ for example. This leads to significantly milder smoothing of high frequency information than would occur with classical Gaussian smoothing where $p=1$. Second, the progressive time evolution of the diffusion process can be monitored, and the “slow motion” suite of gradually smoother images, such as Figure 13 can be stored. This provides an audit trail that allows retrieving possibly useful information that might have been lost in transit to the user-selected optimal image. Different values of the exponent p can be explored.

As shown in Figure 14, such independent and fully reproducible enhancements provide a valuable frame of reference that may be helpful in informing, complementing, and possibly validating the forensic Photoshop methodology.

This work was sponsored by the 2012 NIST Forensic Measurement Challenges grant, “Metrics for Manipulation and Enhancement of Forensic Images.” A NIST Invention Disclosure covering this work was filed by the NIST Technology Partnership Office in May 2013.

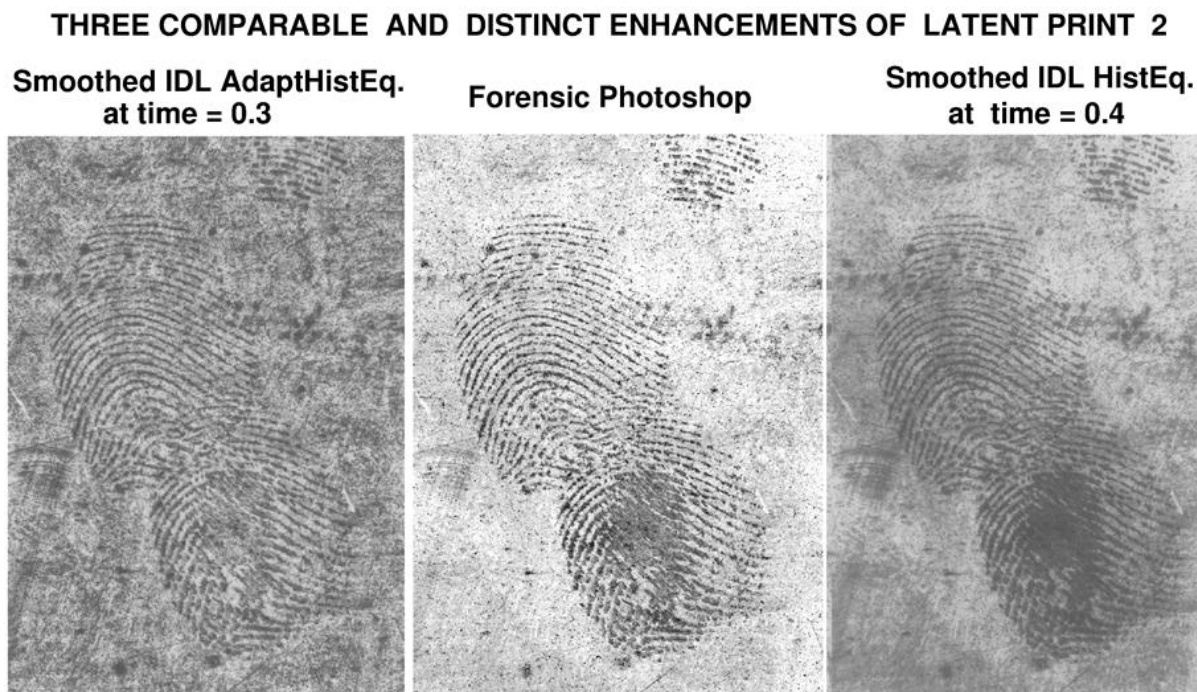


Figure 14. Viewed on-line on high resolution monitor, smoothed IDL images complement and inform the forensic Photoshop image. Leftmost IDL Adaptive Histogram image shows writing near top, streaks near bottom left edge, and horizontal left to right smearing of lower print near lower right corner, in addition to well-defined ridge structure. To a lesser extent, these features are also present in the rightmost IDL Histogram image. However, when the Photoshop image is viewed in isolation, the smearing in the lower print is not immediately evident. Also, the streaks are faint in the middle image, and the writing near the top appears to have been erased.

References

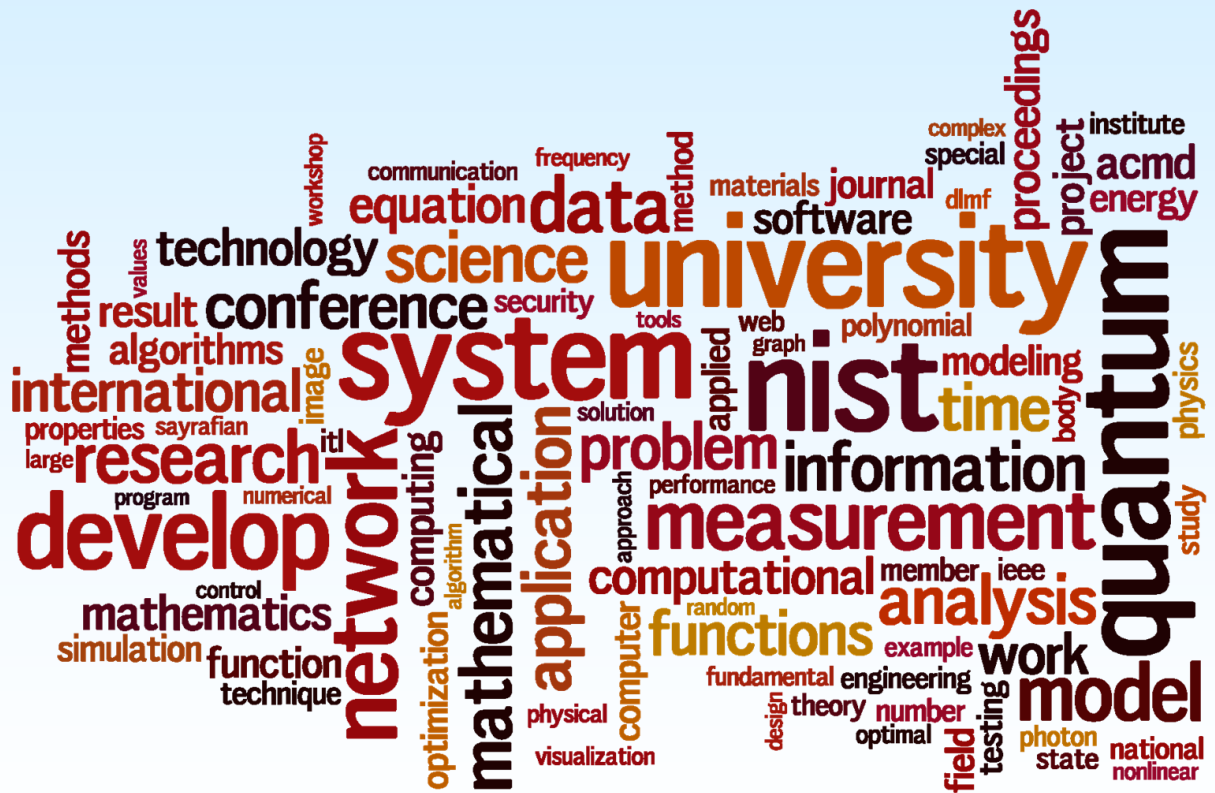
- [1] J. L. Mnookin, A Blow to the Credibility of Fingerprint Evidence, *Boston Globe*, February 2, 2004.
- [2] J. L. Mnookin, The Achilles Heel of Fingerprints, *Washington Post*, May 29, 2004.
- [3] F. McRoberts and S. Mills, Digitized Prints Can Point Finger at the Innocent, *Chicago Tribune*, January 3, 2005.
- [4] F. McRoberts and S. Mills, US Seeks Review of Fingerprint Techniques, *Chicago Tribune*, February 21, 2005.
- [5] J. L. Mnookin, The Courts, the NAS, and the Future of Forensic Science, *Brooklyn Law Review* **75** (2010), 1209-1241.
- [6] Latent Print Examination and Human Factors: Improving the Practice through a Systems Approach, Report of the Expert Working Group on Human Factors in Latent Print Analysis, US Department of Commerce, National Institute of Standards and Technology, (February 2012).
- [7] A. S. Carasso, Alternative Methods of Latent Print Enhancements and Metrics for Comparing Them, NIST Internal Report 7910, January 2013.
- [8] A. S. Carasso, The Use of “Slow Motion” Levy Stable Fractional Diffusion Smoothing in Alternative Methods of Latent Finger Print Enhancements, NIST Internal Report 7932, April 2013.
- [9] Image Processing Toolbox User's Guide (2012), The MathWorks, Inc. Natick, MA 0176.
- [10] ITTVIS Interactive Data Language (IDL), <http://www.exelisvis.com/IDL.aspx>.
- [11] PV-Wave 7.5 Image Processing Toolkit User's Guide, Visual Numerics, Inc. Houston, TX 77042.
- [12] W. K. Pratt, *Digital Image Processing*, Wiley-Interscience, New York, 2012.
- [13] A. S. Carasso and A. E. Vladar, Fractional Diffusion, Low Exponent Levy Stable Laws, and “Slow Motion” Denoising of Helium Ion Microscope Nanoscale Imagery, *Journal of Research of the National Institute of Standards and Technology* **117** (2012).

Participants

A. Carasso (ACMD)

Part III

Project Summaries



Mathematics of Metrology

Mathematics plays an important role in the science of metrology. Mathematical models are needed to understand how to design effective measurement systems, and to analyze the results they produce. Mathematical techniques are used to develop and analyze idealized models of physical phenomena to be measured, and mathematical algorithms are necessary to find optimal system parameters. Finally, mathematical and statistical techniques are needed to transform the resulting data into useful information. Our goal is to develop fundamental mathematical methods and analytical tools necessary for NIST to continue as a world-class metrology institute, and to apply them to critical measurement science applications.

Compensating Operators and Stable Time Marching in Ill-Posed Nonlinear Evolution Equations

Alfred Carasso

See feature article, page 17.

Analysis for Dynamic Metrology

Andrew Dienstfrey
Paul Hale (NIST PML)

See feature article, page 26.

A Framework for Reproducible Latent Fingerprint Enhancements

Alfred Carasso

See feature article, page 29.

Improved Time Delay Estimation Method in the Frequency Domain

Anthony J. Kearsley
Ismet Sahin (University of Maryland)
Marwan Simaan (University of Central Florida)

Time-delay estimation is crucial in many applications such as in seismology, radar, sonar systems, and biomedical sciences [1]. In these applications, multiple noisy copies of a reference waveform are recorded at different times, and time-delay amounts between these recordings provide important information about the underlying system. For instance, in seismology, time-delays between multiple seismic waveforms indicate depths of reflections and propagation velocities of

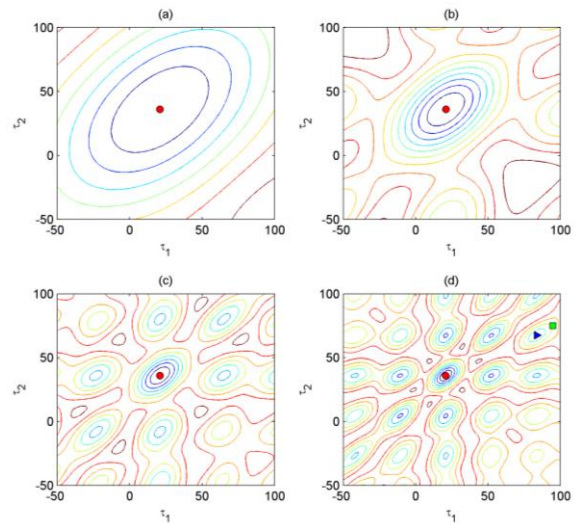


Figure 15. Contours of the cost function for a 2-dimensional time-delay estimation problem. The cost functions with the contours shown in (a), (b), (c), and (d) are successively minimized in this order. Notice the gradual reduction in the basin of attraction. The minimizer of the previous cost function is used as the best initial guess for the current minimization at hand. In (d) the square marker represents the initial guess, the triangle represents the minimizer of the original cost function and the circle represents the minimizer obtained by successive minimizations.

seismic signals through different layers of the earth. These, in turn, reveal structural properties of the sub-surface layers [2]. In sonar and radar systems, time-shifts between transmitted and received waveforms provide estimated location and velocity of an aircraft or an underwater vehicle [1]. In biology, estimation of time delays between multiple potential waveforms is the first step for accurately quantifying amplitude and latencies of brain responses to visual stimuli [3]. Such amplitude and latency measurements are important for diagnosing medical problems such as multiple sclerosis and optic neuritis.

Methods that involve processing signals either in the time domain or in the frequency domain for estimating the time delays have been investigated extensively in the past. Our interest centers on a frequency domain method that has been proven to be very successful in estimating time delays to within a fraction of the sampling period. This method formulates and

minimizes a frequency domain cost function which takes into account spectral differences between the phase-shifted discrete Fourier transforms (DFTs) of all pairs of the available signals [2]. A limiting factor in this approach is its sensitivity to the initial guesses of time-delays which are provided to the optimizers. Optimization methods tend to diverge for initial guesses that are not near to the minimizer due to the narrow basin of attraction of the cost function.

Since a good initial guess may not be available for many applications, we aim to find approaches that are in general not sensitive to the choice of initial guesses. To this end, we derive the analytic Hessian of the cost function and obtain a condition guaranteeing the positive definiteness of the Hessian, and therefore convergence of second order optimization algorithms such as Newton's algorithm [4]. This condition motivates us to construct multiple modified cost functions, minimizing them successively in order to have larger basins of attraction at the beginning, and then gradually reducing the size of the basin.

Figure 15 illustrates this process. Figure 15 (a) has the largest basin of attraction whose minimization from far-initial points leads to a convergence to a point that is in the basin of the true minimizer. The converged point becomes the initial guess for the next minimization task involving the cost contours in Figure 15 (b). Proceeding this way, we converge to the true minimizer represented by the circle marker in Figure 15 (d) from the initial square point. Note that minimization of the original cost function shown in Figure 15 (d) would result in convergence to the nearest local minimizer shown by the triangle marker, which is far from the global optimum.

We are planning to develop more efficient numerical algorithms in order to improve scalability of this approach for large dimensional time-delay estimation problems in a future work.

- [1] G. Clifford Carter, *Coherence and Time Delay Estimation: An Applied Tutorial for Research, Development, Test, and Evaluation Engineers*, IEEE Press, 1993.
- [2] M. Simaan, A Frequency-Domain Method for Time-Shift Estimation and Alignment of Seismic Signals, *IEEE Transactions on Geoscience and Remote Sensing* **GE-23:2** (March 1985), 132–138.
- [3] I. Sahin and N. Yilmazer, A Discrete Fourier Transform Method for Alignment of Visual Evoked Potentials, in *Proceedings of the IEEE Symposium on Computational Intelligence in Bioinformatics and Computational Biology (CIBCB)*, May 2010, 1-3.
- [4] I. Sahin, M. Simaan, and A. J. Kearsley, A Globally-Convergent Time Delay Estimation Method in Frequency Domain, in review.

Applied Hierarchical Control

Anthony J. Kearsley

Very often systems governed by partial differential equations (PDE) can be controlled (e.g., through boundary control or distributed control). One has the ability to select boundary conditions or prescribe state equation variables to behave in a particular way. These problems are particularly challenging when the PDE are time dependent. These types of problems abound in applications, especially those in measurement science. Efficient numerical methods for the solution of these problems have been the subject of significant research [1]. Recently, specialized numerical methods have been developed for application-specific problems. Such is the case with, for example, calibration of spectrometry instruments.

Motivated by specific scientific and engineering applications, such as those arising in calibrating and optimizing instrument performance, we investigate a means of formulating a class of optimal control problems in which desired behavior of solutions or “targets” can be partitioned into categories of increasing relative importance. For example, one might want to find instrument settings that reduce the signal-to-noise in a portion of a spectrum, while simultaneously optimizing a known absolute molecular mass distribution. These instrument response function problems are notoriously difficult, and casting them as hierarchical control problems, problems with multiple objectives, appears to be a fruitful research direction.

There is no unique mathematical formulation of these types of problems; indeed, different formulations can generate completely different “optima.” In one formulation, the problem is posed as the minimization of a weighted sum of the deviations from the targets with weights corresponding to an established priority among the targets (see [6]). Another formulation, sometimes referred to as goal programming, insists that a set of preferred targets be satisfied to within certain tolerances and the others be reduced as much as possible within these constraints (see [5]). Both of these approaches involve the choice of a set of weights or tolerances for which there may be little theoretical guidance.

An instance of this problem occurs, for example, in calibrating a matrix-assisted laser desorption/ionization time-of-flight (MALDI/TOF) mass spectrometer when one knows the total amount of compound present in a sample, suggesting that one minimize a least squares or distance regression function while simultaneously maximizing the signal to noise ratio. Motivated by this application, and others, we seek to formulate this problem as a collection of nested optimization problems in which the solutions of the inner problems are determined using the variables

in the outer problems as parameters. This approach, which is based on the work of von Stackelberg [4] in an economics context, requires that the deviations from the least important targets, called the “follower” targets, be decreased only after the deviations from the most important targets, called the “leader” targets, satisfy prescribed bounds. This type of optimal control problem has been termed *hierarchical control* [2]. One way of formulating this type of problem is in terms of a nested optimization structure in which, in an “inner minimization,” the follower targets are minimized subject to fixed values of certain of the control variables, and then an “outer minimization” is performed over the remaining control variables to obtain optimal leader target satisfaction [3]. The resulting accuracy on the follower targets is therefore determined by, and is subordinate to, the optimization over the leader targets. In the case of MALDI/TOF calibration, matching known experiment parameters would be a primary objective, and maximizing signal to noise a secondary or “follower” objective.

Recently we have derived optimality conditions for a linear differential equation [7] and are very close to extending our results to a more general reaction diffusion equation [8]. This work constitutes significant steps towards the ultimate goal of robustly and reproducibly optimizing instrument performance for multiple objectives.

- [1] R. Glowinski, J. L. Lions and J. He, *Exact and Approximate Controllability for Distributed Parameter Systems: A Numerical Approach*, Cambridge University Press, 2008.
- [2] J. L. Lions, Hierarchical Control, *Proceedings of the Indian Academy of Sciences (Mathematical Sciences)* **104:1** (February 1994), 295-304.
- [3] L. Vicente and P. Calamai. Bilevel and Multilevel Programming: A Bibliography Review, *Journal of Global Optimization* **6** (1994), 1–16.
- [4] H. von Stackelberg, *Marktform und Gleichgewicht*, Springer, Vienna, 1934.
- [5] J. P. Ignizio, *Goal Programming*, Lexington Books, Lexington MA, 1976
- [6] J. Koski, H. Eschenaur and A. Osycka, *Multicriteria Design Optimization*, Springer-Verlag, Berlin, 1990.
- [7] A. J. Kearsley Optimality Conditions for the Hierarchical Control of a Linear Partial Differential Equation, in *Proceedings of the 2nd IEEE Conference on Instrumentation, Control and Automation*, November 2011.
- [8] A. J. Kearsley, Hierarchical Control of a Reaction Diffusion Equation, *International Journal on Applied Mathematics and Statistics* **35:5** (2013), 5–19.

Molecular Movies: Imaging Femtosecond Motion during Electrochemical Transitions

Bradley Alpert

Joel Ulom (NIST PML)

Chris Cromer (NIST PML)

Ralph Jimenez (NIST PML)

Vital to the development of next-generation nanomaterials, including photovoltaics and industrial catalysts, is an understanding gained through measurement of electron release, transport, and transfer in engineered nanostructures. This project, supported for the past three years by a NIST Innovations in Measurement Science (IMS) grant, proposes a revolutionary, table-top x-ray imaging system to capture the motion of electrons, atoms, and molecules on femtosecond time scales and with picometer spatial resolution.

The combination of table-top x-ray lasers, a dramatic recent breakthrough developed at JILA¹¹, with transition-edge sensor (TES) microcalorimeter spectroscopy, developed and refined in the NIST Quantum Electronics and Photonics Division, promises to enable these new measurement capabilities. The integration of these components, accompanied by significant increase in detector array sizes, to achieve large increases in temporal and spatial resolution while maintaining extraordinary TES energy resolution, requires new data modeling and processing techniques. These techniques will overcome current limitations by

- Resolving temporal overlap in photon detection while achieving energy resolution of temporally isolated arrivals,
- Improving efficiency in elimination of low-frequency background noise, and
- Extending multiplexing and reducing cross talk in extracting the signals from 0.1 K to room temperatures.

Wiener filtering, long used among astronomers for estimating amplitudes of pulses of known shape contaminated with noise of known frequency content, is suitable for measuring isolated pulses. Novel processing approaches are being developed and characterized that rely on this knowledge, but are suitable for overlapping pulses.

This year progress occurred in the following areas:

1. Alpert's method for computing filters in the time domain, rather than the frequency domain, allowing for orthogonality to prior pulse tails, and its evaluation on gamma-ray data, was published [1]. It is being implemented at Los Alamos National

¹¹ JILA is a physics research institute jointly operated by NIST and Colorado University at Boulder.

Laboratory to accelerate an extensive data collection being taken to evaluate the effectiveness of microcalorimeters, as an alternative to high-purity germanium detectors, for determining isotopic composition of nuclear materials. It is also being implemented at NASA Goddard Space Flight Center to evaluate as a processing technique for X-ray spectroscopy data. Consultations with both of these external groups are ongoing.

- An extensive data collection from special preparations by Japanese collaborators of several different elements (Ti, Cr, Mn, Fe, Co in one set) was made at NIST of X-ray emissions from electronic transitions, with more than 100 detectors operating in parallel, with multiplexing, to further evaluate processing and calibration challenges. One issue that rose in prominence is the dependence of photon pulse shape on subsample arrival phase and the corresponding filtering sensitivity to pulse arrival phase. Alpert has worked with Joe Fowler of the NIST Physical Measurement Laboratory to propose and evaluate new processing techniques to cope with this issue.

The new experimental apparatus that couples the pulsed x-ray laser with a large microcalorimeter array has, over the past year, been used to collect extensive data sets. As anticipated, several new processing issues have become prominent, including detector crosstalk, detector nonlinearity, and non-Gaussian noise patterns. For some of these, it appears most expedient to treat them with new processing methods yet to be developed.

- B. K. Alpert, R. D. Horansky, D. A. Bennett, W. B. Doriese, J. W. Fowler, A. S. Hoover, M. W. Rabin and J. N. Ullom, Operation of Gamma-Ray Microcalorimeters at Elevated Count Rates using Filters with Constraints, *Review of Scientific Instruments* **84:5** (2013), 056107.
- B. K. Alpert, W. B. Doriese, J. W. Fowler and J. N. Ullom, Predicted Energy Resolution of a Running-Sum Algorithm for Microcalorimeters, *Journal of Low Temperature Physics* **167:5-6** (2012), 582-587.
- W. B. Doriese, B. K. Alpert, J. W. Fowler, G. C. Hilton, A. S. Hojem, K. D. Irwin, C. D. Reintsema, D. R. Schmidt, G. M. Stiehl, D. S. Swetz, J. N. Ullom and L. R. Vale, Optimization of the TES-Bias Circuit for a Multiplexed Microcalorimeter Array, *Journal of Low Temperature Physics* **167:5-6** (2012), 595-601.
- D. A. Bennett, R. D. Horansky, D. R. Schmidt, A. S. Hoover, R. Winkler, B. K. Alpert, J. A. Beall, W. B. Doriese, J. W. Fowler, C. P. Fitzgerald, G. C. Hilton, K. D. Irwin, V. Kotsubo, J. A. B. Mates, G. C. O'Neil, M. W. Rabin, C. D. Reintsema, F. J. Schima, D. S. Swetz, L. R. Vale and J. N. Ullom, A High Resolution Gamma-Ray Spectrometer Based on Superconducting Microcalorimeters, *Review of Scientific Instruments* **83:9** (2012), 093113.

Stochastic Simulation in Chemical Spectroscopy

Anthony Kearsley

William Wallace (NIST MML)

Yutheeka Gadhyan (University of Houston)

In the data analysis of chemical spectra a collection of deterministic numerical schemes are used together to predict chemical information. Very often linear regression or “binning” of data is used in conjunction with a derivative checker that finds peaks and troughs. This process is fraught with difficulties, and is very often performed by a technician by eye. This is, of course simply impossible in many applications (e.g., medicine, forensics) where an automated procedure is necessary for the instrument output to be credible.

Recently we have begun examining the use of stochastic differential equations (SDE) to model and build regression simulations of chemical spectra. Very loosely, one can construct an SDE that has two components, a drift component that captures the signal, and a diffusion term that captures the noise. In so doing, the SDE naturally (and automatically) can split the “instrument output” into noise and true signal. Once this has been accomplished, one can find peaks, examine structures, measure the area under structures, etc. These techniques are quite often used in financial modeling, albeit in a different way.

This year we developed such a scheme and analyzed its convergence and statistical properties. Using a first order *Euler-Maruyama* discretization, one can build an inexpensive numerical scheme to regress on chemical spectra accurately. In addition, statistical information about the noise estimation can be calculated inexpensively. To validate these ideas we derived and analyzed the SDE, implemented a simple numerical integration, together with associated convergence anal-

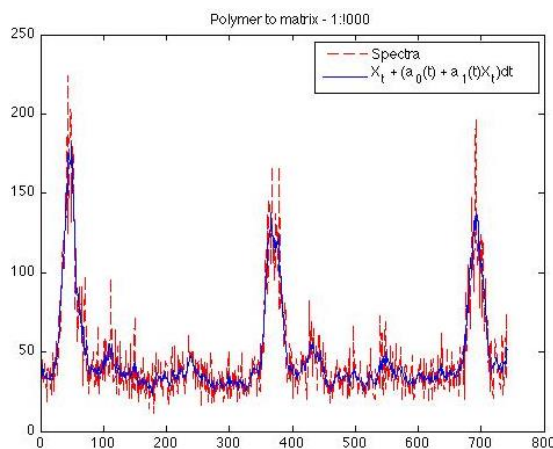


Figure 16. Regression applied to a data spectrum from a MALDI-TOF mass spectrometry study of a narrow-polydispersity synthetic polymer.

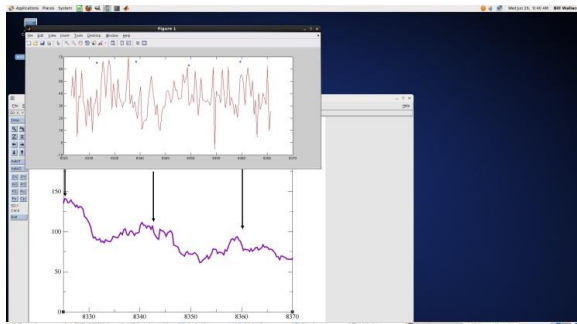


Figure 17. Results of off-the-shelf peak picking software.

ysis, which suggested a time-stepping scheme. We applied the regression to a data spectrum from a MALDI-TOF mass spectrometry study of a narrow-polydispersity synthetic polymer. Polystyrene, with an average molecular mass of 9100 g/mol, was analyzed using all-trans-retinoic acid as a matrix, and silver trifluoroacetate as a cationizing agent, as detailed in [1]. Early results appear promising (see Figure 16); the regression certainly follows the instrument output well, and it succeeds in automatically separating noise from signal.

Because this regression provides a statistical estimate of the noise, one has the ability to interrogate peaks in the spectrum, that is, to examine the estimated noise in a neighborhood of a peak that was identified by, for example, the peak peaking software from the instrument. In Figure 17 we see an interesting example where off-the-shelf peak-picking software found four peaks very close to each other. The magnitude of these peaks was suspiciously low. Examining the noise estimate produced by the SDE approach, three of the four identified peaks were below the level of the noise, suggesting that the off-the-shelf software incorrectly identified them as peaks. However, one of the peaks was above the estimated noise level. Surprisingly, this fourth peak was a *true* peak, thus illustrating the potential benefit of our SDE regression approach. A preliminary manuscript is being prepared [2].

- [1] C. M. Guttman, K. M. Flynn, W. E. Wallace and A. J. Kearsley, Quantitative Mass Spectrometry and Polydisperse Materials: Creation of an Absolute Molecular Mass Distribution Polymer Standard, *Macromolecules* **42** (2009), 1695–1702.
- [2] Y. Gadhyan, A. Kearsley and W. Wallace, Stochastic Regression Modelling of Chemical Spectra, in preparation.

Computational Tools for Shape Measurement and Analysis

Gunay Dogan

The main goal of this project is to develop efficient and reliable computational tools to detect geometric structures and to evaluate and compare them in a quantitative manner. Such structures include curves, regions and boundaries obtained from given direct and indirect measurements, such as microscope images or tomographic measurements. This is important in many areas of science and engineering, such as the analysis of microscopy images for cell biology or micro-CT (computed tomography) images of microstructures in material science.

We have been developing image segmentation algorithms based on energy minimization principles, which leads to shape optimization formulations. In this approach, the user starts the segmentation algorithm with some initial estimate of the sought region boundaries, which is then deformed or evolved iteratively towards minimal energy configurations, which are, by design, the right segmentations. An example of such a process is shown in Figure 18.

Segmentation of different image classes requires different model energies specially designed for each class. For example, a two-phase-material image can be segmented by the Chan-Vese segmentation energy, which decomposes the image into a background and some foreground objects. This was implemented previously as part of this project. In this fiscal year, this model was extended to handle multiphase images as well. Images with well-defined edges, on the other hand, can be segmented with the Geodesic Active Contour (GAC) model, also implemented as part of this project. The GAC model is sensitive to the choice of image interpolation and image derivatives. To ensure robustness and efficiency, B-splines were incorporated into the image definition. Moreover, a diffusion process was implemented on the image grid to obtain smooth image features to be used by the segmentation models. An anisotropic version of the GAC model was also developed. This takes local orientation of the candidate boundaries into account to improve alignment with the target boundaries. New geometric function definitions were implemented to support definitions of the new energies mentioned, as well as future energies.

Significant efforts have gone into increasing the efficiency and robustness of the shape optimization framework. Ideally, the segmentation algorithm should terminate successfully in a short amount of time and not require a lot of user tuning. In order to reduce computation time, judicious caching was introduced for both shape energies and mesh functions, so that numerical quantities would be computed only at the mesh locations needed and only when they were new

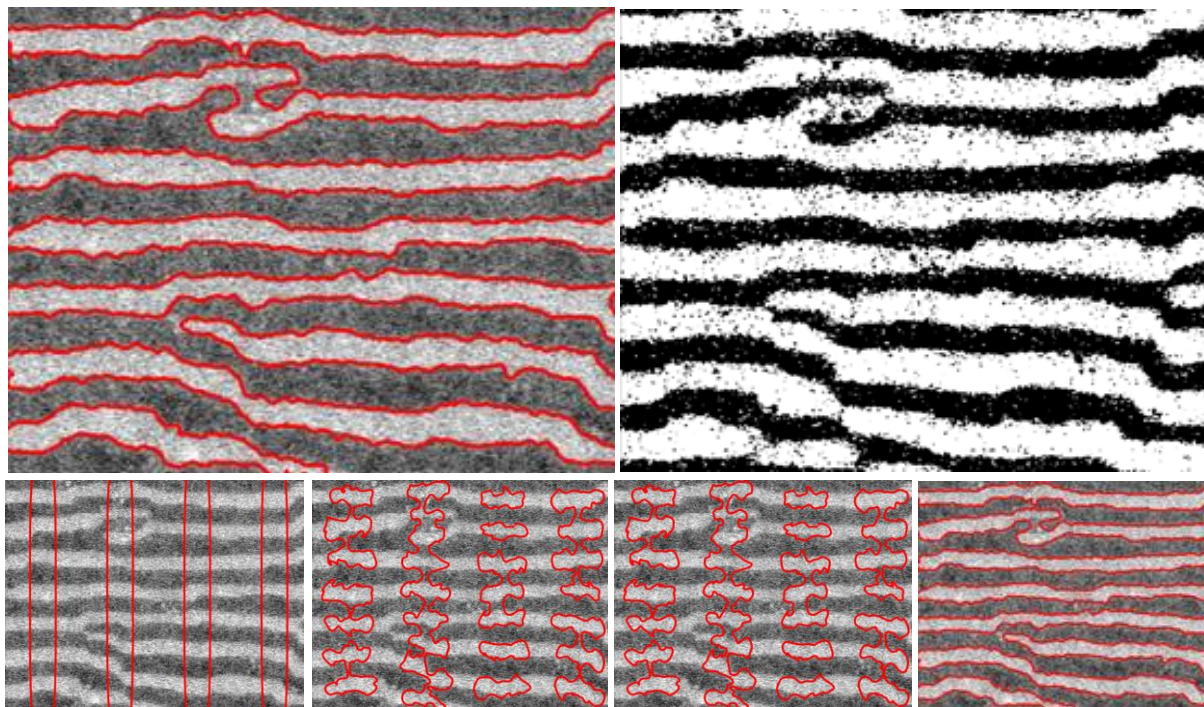


Figure 18. The segmentation of a microstructure image using the algorithms developed in this project. The top left image shows the final result of our segmentation, which produces well-defined regions and boundaries. It compares favorably with the result on top right, which was obtained by thresholding, a very common technique used for image segmentation. Thresholding does not work well for such noisy images and produces many misclassified pixel labels, i.e. black dots in white areas and white dots in black areas. This is not a problem for our algorithm. The bottom row shows some intermediate steps of the iterative segmentation process. The curves on the left image are the starting curves. The algorithm deforms them gradually as shown in the intermediate steps, and it stops when the curves are aligned with region boundaries as shown in the last image of the bottom row.

and needed to be refreshed. Additionally, sophisticated line search algorithms were implemented to reduce both the number of iterations and energy evaluations. Finally, automatic stopping criteria were developed to avoid premature termination and superfluous iterations once the segmentation is achieved.

Some preliminary work to address the case of indirect measurements (tomography) was carried out. Such reconstructions can be also formulated as a shape optimization, which fits our framework. A simple proof of concept for the case of x-ray tomography was implemented to demonstrate viability. A potential application is reconstruction of microstructure interfaces from micro-CT measurements.

Computation of Shape Geodesics

Gunay Dogan

Javier Bernal

Charles Hagwood (NIST ITL)

Shape, a natural and intrinsic attribute of geometric structures and objects, is a very good comparator. Its use in applications, e.g., object recognition, cluster and classification analyses, computational biology, analysis

of microstructure grains, and other areas, attests to its significance for modern technology. Many years of work on shape analysis by contributors such as Bookstein, Kendall, Grenander, Younes, and Mumford, culminated in work by Srivastava et al. [1], who derived a presentation of shape as an object in a Riemannian manifold. With such a representation, geometric objects can be compared in a quantitative manner based on their geodesic distance.

The development of a fast algorithm for computing shape geodesics is under way. Such an algorithm is essential for large-scale comparisons. For this purpose, proper optimality conditions have been derived for the minimization problem at the heart of the shape geodesics computation. Using this formulation, unnecessary steps in Srivastava's algorithm have been removed. This has resulted in savings in computation time on synthetic examples. Moreover, geodesic distance values on these synthetic examples have been improved. These results are preliminary, but encouraging, confirming that the work in this area is moving in the right direction. See Figure 19.

- [1] E. Klassen, A. Srivastava, W. Mio and S. Joshi. Analysis of Planar Shapes using Geodesic Paths on Shape Spaces, *IEEE Pattern Analysis and Machine Intelligence* **26:3** (March 2004), 372-383.

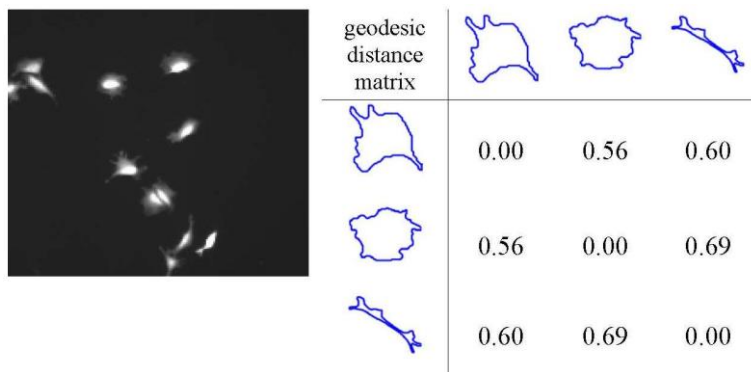


Figure 19. Left: fluorescence image of multiple DLEX-p46 cells. Right: A geodesic distance comparison matrix showing distances between 3 cell shapes. In real comparison problems, 100 x 100 geodesic matrices or larger are required. This is why improved computation speed is needed.

Traceable Simulation of Magnetic Resonance Imaging

Zydrunas Gimbutas

Andrew Dienstfrey

Steve Russek (NIST PML)

Katy Keenan (NIST PML)

Karl Stupic (NIST PML)

Magnetic resonance imaging (MRI) is maturing as a quantitative biomedical imaging technology. For example, imaging facilities routinely report tumor volumes in units of mm^3 , blood perfusion in units of $\text{ml g}^{-1} \text{min}^{-1}$, apparent diffusion coefficient in $\text{mm}^2 \text{s}^{-1}$, and temperature in K. However, as of a few years ago the use of SI units for these technologies was potentially unwarranted as SI traceability chains supporting these MRI measurement modalities were unclear and, in many cases, non-existent. More recently NIST and partner institutions have made substantial investments to develop such traceability chains. NIST now supports several *phantoms*, as standard reference artifacts are referred to in the medical community, enabling SI-traceable calibration for MRI scanners.

MRI is predicated on established physical principles. It follows that predictive quantitative simulation of this imaging modality is possible, and a growing number of computer codes are available which claim to do just this. Virtual prototyping is highly desirable to improve the fundamental understanding of MRI capabilities, with expectations for significant reductions in time and costs by comparison with use of physical scanners. While nearly all agree on the potential for quantitative MRI simulation, neither NIST nor any other national metrology institution is currently positioned to verify the accuracy of such claims.

In 2013 we initiated a new project to create SI-traceable simulations for magnetic resonance imaging. Under this project we will develop quantitative analysis of MRI simulation side-by-side with the ongoing MRI phantom development projects at NIST. This past year we obtained, compiled, and executed a number of MRI simulation codes. These are large codebases developed principally within academic and industrial research labs, and they carry minimal documentation. Regardless, we can now execute a number of the most highly-cited MRI simulation tools: Object-Oriented Development Interface for NMR (ODIN) [2], SIMRI [1], and JEMRIS [3].

In the next year we will continue to explore the quantitative capabilities of each code in isolation, as well as identify MRI measurement scenarios that will allow cross-comparison of the numerical outputs. In tandem, we will collaborate with NIST researchers performing MRI measurements to begin comparing computational to experimental results. In the long-term, we hope to further enable simulation-based innovations in MRI imaging and future phantom design, while maintaining traceability to NIST physical measurements, and the International System of Units.

- [1] H. Benoit-Cattin, G. Collewet, H. Saint-Jaimes and C. Odet, The SIMRI Project: a Versatile and Interactive MRI Simulator, *Journal of Magnetic Resonance* **173:1** (March 2005), 97-115.
- [2] T. H. Jochimsen and M. von Mengershausen. ODIN - Object-oriented Development Interface for NMR, *Journal of Magnetic Resonance* **170:1** (Sept. 2004), 67-78.
- [3] T. Stöcker, K. Vahedipour and D. Pufgelder, High-Performance Computing MRI simulations, *Magnetic Resonance in Medicine* **64:1** (July 2010), 186-193.

Modeling and Optimization in Cryobiology

Anthony Kearsley

Daniel Anderson (George Mason University)

James Benson (Northern Illinois University)

Adam Higgins (Oregon State University)

Mathematical modeling plays an important role in understanding the behavior of cells, tissues, and organs undergoing cryopreservation. Uses of these models range from explanation of phenomena, exploration of potential theories of damage or success, development of equipment, and refinement of optimal cryopreservation and cryoablation strategies. Cryopreservation

procedures permit cells to be stored indefinitely using extremely cold temperatures, suspending metabolic activities, and preserving the cell and its function.

Loosely speaking, there are two main types of cryopreservation procedures: equilibrium (conventional slow freezing) and non-equilibrium or ultra-rapid freezing (vitrification). Both procedures employ the use of cryoprotectants, chemicals behaving like antifreeze. Cryoprotectants prevent cellular damage during the freezing process. After proper freezing, cells should be able to be stored for an indefinite amount of time. This can be done, for example, by immersing them in liquid nitrogen, an extremely cold fluid with an approximate temperature of -196° C. Cryoprotectants must be removed during the thawing process; slowly the water balance in the cell is restored and normal activity in the cell should return.

Procedures exist for the freezing of single cells, tissue comprised of many cells and entire organs. Size, amount of cytoplasm (or fluid), and structural complexity change the freezing procedures employed. For example, cells with less cytoplasm, like sperm cells, are generally considered to be less difficult to freeze than those cells with more cytoplasm, like eggs. Slow freezing or equilibration has been successfully employed to freeze and store a wide range of cells but research is ongoing to optimize the process.

Recently we studied the use of optimization techniques to determine or improve the equilibration of cryoprotectant. We considered the case of cells and tissues with high concentrations of permeating chemicals known as cryoprotective agents, or CPAs. Despite their protective properties, CPAs can cause damage as a result of osmotically-driven cell volume changes, as well as chemical toxicity. In this study, data was used to determine a toxicity cost function, a quantity that represents the cumulative damage caused by toxicity. We then used this cost function to define and numerically solve the optimal control problem for CPA equilibration, using human oocytes as a representative cell type with high clinical relevance. The resulting optimal procedures are predicted to yield significantly less toxicity than conventional procedures.

Results showed that toxicity is minimized during CPA addition by inducing the cell to swell to its maximum tolerable volume and then loading it with CPA while in the swollen state. This counterintuitive result is considerably different from the conventional step-wise strategy, which involves exposure to successively higher CPA concentrations in order to avoid excessive shrinkage. The procedures identified are a first step deriving procedures that significantly reduce damage due to toxicity.

Over the last half century there has been a considerable amount of work in bio-heat and mass-transport, and these models and theories have been readily and repeatedly applied to cryobiology with much success.

However, there are significant gaps between experimental and theoretical results that suggest that there are missing links in models. One source for these potential gaps is that cryobiology is at the intersection of several very challenging aspects of transport theory: it couples multi-component, moving boundary, multiphase solutions that interact through a semipermeable elastic membrane with multicomponent solutions in a second time-varying domain, during a two-hundred Kelvin temperature change with multi-molar concentration gradients and multi-atmosphere pressure changes.

We have been developing mathematical and computational models built on first principles to describe coupled heat and mass transport in cryobiological systems in an effort to account for these various effects. Our efforts have advanced along three fronts: (1) we have examined concentration variable relationships, their impact on choices Gibbs energy models, and their impact on chemical potentials, (2) we have subsequently developed heat and mass transport models that are coupled through phase-change and biological membrane boundary conditions, and (3) we have developed numerical methods for solving these multi-species multiphase free boundary problems.

- [1] D. M. Anderson, J. D. Benson and A. J. Kearsley, Foundations of Modeling in Cryobiology, in preparation.
- [2] J. D. Benson, A. J. Kearsley and A. Z. Higgins, Mathematical Optimization Procedures for Cryoprotectant Equilibration using a Toxicity Cost Function, *Cryobiology* **64:3** (2012), 144-151.

Equilibrium and Stability of Drops on a Conical Substrate

Asha Nurse,
Sean Colbert-Kelly
Geoffrey McFadden
Sam Coriell (NIST MML)

In some applications of tissue engineering, biological cells in solution show a tendency to self-assemble into a spherical cluster, a configuration that minimizes the surface area of the assembly. If the cells are situated in the bottom of a scaffold that contains a conical pillar, they can instead be forced to form a toroidal cluster at the base of the pillar as shown in Figure 20.

Depending on the size of the cluster, the cells are sometimes observed to climb the side of the pillar, in the direction opposed to gravity, eventually reaching the apex of the cone and falling off. A dynamical model of this process has been developed by A. Nurse et al. [1, 2], in which the motion results from the competition between the effects of gravity and surface energy of the cluster. In a toroidal geometry with given volume, the cluster can reduce its total surface area by decreasing



Figure 20. Side view of a toroidal cell cluster climbing the side of a conical pillar.

its major radius, which it can do if it climbs the side of the pillar. This motion reduces the net surface energy at the expense of the gravitational potential energy, which tends to oppose the upward motion.

We have continued this modeling effort by studying the equilibrium and stability of toroidal liquid drops on a conical substrate, taking into account the effects of gravity and surface energy. Axisymmetric configurations can be computed by minimizing an appropriate energy functional that depends on the shape of the drop, resulting in a nonlinear ordinary differential equation coupled to a volume constraint. The solution depends on the cone geometry, the contact angle of the drop on the substrate, the drop volume, and the ratio of gravitational to capillary forces as measured by the Bond number $Bo = \rho g R^2 / \gamma$, where ρ is the drop density, g is the gravitational acceleration, R is the radius of a sphere of equal volume, and γ is the

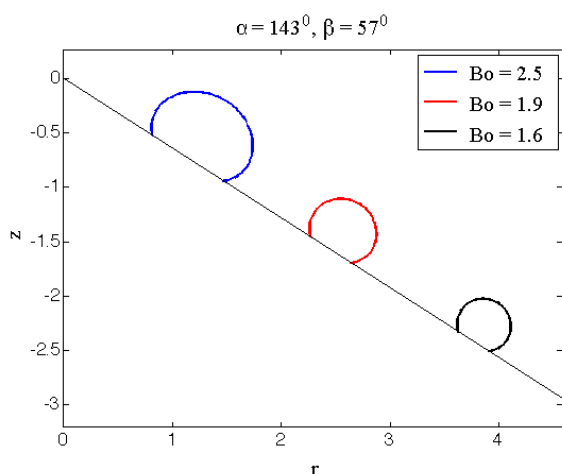


Figure 21. Equilibrium cross-sections of three axisymmetric liquid drops on the side of a conical pillar with half-angle $\beta = 57^\circ$ at the apex of the cone. The drops have contact angles of $\alpha = 143^\circ$ on the conical substrate. Drops corresponding to three different Bond numbers Bo are shown, where the Bond number is the ratio of gravitational to capillary forces.

surface energy. Examples of equilibrium shapes are shown in Figure 21.

Rather surprisingly, increasing the Bond number (stronger gravity) results in drops that are higher on the cone, not lower. This results from the requirement of an equilibrium force balance: a larger capillary force is produced if the drop moves up and reduces its major radius. Conservation of volume produces an increase in the drop's minor radius as the major radius decreases.

Axisymmetric toroidal drops can also be subject to instabilities that can cause “fluting” in the azimuthal direction that are analogous to the Raleigh instability of a liquid jet, which can lead to breakup of the jet via droplet formation. We have therefore also formulated the associated stability problem, which involves a solution of the equations for the second variation of the energy functional. We find that the drops are subject to a non-axisymmetric instability to perturbations that can cause tilting and distortion of the drop.

- [1] A. Nurse, L. B. Freund and Jacquelyn Youssef, A Model of Force Generation in a Three Dimensional Toroidal Cluster of Cells, *Journal of Applied Mechanics* **79** (2012), 051013.
- [2] J. Youssef, A. Nurse, L. B. Freund and Jeffrey R. Morgan, Quantification of the Forces Driving Self-Assembly of Three-Dimensional Microtissues, *Proceedings of the National Academy of Sciences* **108** (2011), 6993-6998.

Diffuse Interface Model Incorporating Interfacial Properties

Sean Colbert-Kelly

Geoffrey McFadden

Frederick Phelan, Jr. (NIST MML)

Surfactants are chemical compounds that lower interfacial tension between two liquids or a liquid and a solid. Surfactants have important applications in detergents, droplet break-up, reducing the risk from bubbles formed in blood due to rapid decompression and prevention of lung collapse at the end of expiration [1, 3]. This research project studies the transition that occurs between two immiscible fluids with surfactant at the interface between the two fluids.

Discontinuities in fluid properties at the interface, as well as properties such as surface energy and surface viscosity associated with the interface itself, tend to complicate the computation of flow near the interface. Utilizing a diffuse interface model can be useful in investigating the dynamics near the interface. The mixing properties of the two fluids affect the interface shape's dynamics. Surfactants migrate to the fluid interface in a binary mixture due to the amphiphilic nature of these molecules [1]. The presence of the surfactant produces dramatic changes in the interfacial

properties of the fluid mixture, and therefore greatly alters the stability, equilibrium properties, and the droplet dynamics of the mixture. An initial effect of the surfactant is a lowering of the surface tension. However, gradients in the surfactant concentration on the drop surface under flow give rise to Marangoni forces that alter drop shape, breakup and coalescence dynamics, as well as giving rise to flow induced migration [2]. An additional effect of the surfactant is that they give rise to shear and dilational interfacial viscosities. Along with surface tension, the interfacial viscosities play a crucial role in coalescence dynamics, therefore governing the long time stability of emulsions. Current models do not accurately model the dramatic effects of surfactants on emulsion properties and dynamics.

Following previous work, this project intends to develop a description of the mixture of two immiscible fluids with surfactants where mixing can occur near the interface, while incorporating interfacial properties that many diffuse interface models (DIM) tend to ignore. Previous research has employed a mixing rule to incorporate interfacial viscosity [4]. However, this project will consider alternative approaches using a diffuse interface description. The research project will consider the situation of a droplet in a particular medium that follows a Stokes flow. The two liquids are considered Newtonian and incompressible, where in the interfacial region this assumption may not hold. In addition to developing a diffuse interface model, this project will study the limiting problem of the diffuse interface model, to determine if a sharp interface model is recovered in letting the interfacial region get arbitrarily thin. It will also be of benefit to study the deformation of the droplet, and determine if the droplet will remain spherical in shape.

Currently, we are comparing various free energy formulations to determine which one is to be utilized [1, 3] based on the representation of the system of interest and computational ease. From what has been gathered, the common elements of the free energy are:

- *Cahn-Hilliard free energy*: The bulk energy density drives the system into distinct phases corresponding to its minimum values. The gradient energy term penalizes steep gradients characterized by the constant multiplying this term.
- *Entropy for ideal mixing of surfactant*: This term governs the kinetics of surfactant adsorption and also incorporates the saturation of surfactant at the interface, governing the entropy decrease of mixing the surfactant with the bulk phase [1].
- *Surfactant-interface coupling energy*: This term describes the adsorption behavior of the surfactant near the binary fluid interface [3].
- *Energy for excess surfactant in the pure regions*: This term penalizes the free energy if there is free

surfactant in the bulk region of the system. It can also be regarded in some models as the *bulk solubility* [1]. Some models incorporate the penalization of free surfactant in the pure phases in the surfactant-interface coupling energy term [3].

- [1] S. Engblom, M. Do-Quang, G. Amberg and A.-K. Tornberg, On Diffuse Interface Modeling and Simulation of Surfactants in Two-Phase Fluid Flow, *Communications in Computational Physics* **14:4** (2013), 879-915.
- [2] J. T. Schwalbe, F. R. Phelan, Jr., P. M. Vlahovska and S. D. Hudson, Interfacial Effects on Droplet Dynamics in Poiseuille Flow, *Soft Matter* **7** (2011), 7797-7804.
- [3] C.-H. Teng, I.-L. Chern and M.-C. Lai, Simulating Binary Fluid-Surfactant Dynamics by a Phase Field Model, *Discrete and Continuous Dynamical Systems Series B* **17:4** (2012) 1289-1307.
- [4] W. Yu and C. Zhou, The Effect of Interfacial Viscosity on the Droplet Dynamics Under Flow Field, *Journal of Polymer Science Part B: Polymer Physics* **46:14** (2008), 1505-1514.

Spectral-Galerkin Scheme to Study Ferroelectric Liquid Crystal Properties

Sean Colbert-Kelly
Geoffrey McFadden
Daniel Phillips (Purdue University)
Jie Shen (Purdue University)

This project considers the effect of introducing defects into a ferroelectric liquid crystal thin film. The liquid crystal film of interest is chiral smectic c (SmC*), which has a spontaneous polarization field [1]. Such films are composed of layers of liquid crystal molecules. The local average of the molecular long axes at a point in the layer, the director field \mathbf{n} , is tilted at a constant angle $0 < \theta < \pi/2$ from the normal to the layers. Hence, each layer in a thin film of SmC* can be represented as a two-dimensional liquid [2], with u representing the normalized projection of \mathbf{n} onto the 2D layer.

If a particle is introduced into a thin film SmC* liquid crystal, then an island will form, several layers thicker than the surrounding thin film, around the defect [3]. These islands are disk-like and u is tangential counterclockwise on the island's outer edge, resulting in a vector field of degree 1. Its initial orientation is tangential. However, increase in the island's size or external forces can cause distinct textural transformations in the director field. The pattern can remain unchanged or transform to a *simple spiral*, tangential counterclockwise on the boundary and approximately radial at the smoke particle boundary [3].

The free energy of this system in the island can be described by a relaxed energy

$$E_\epsilon(u) = \frac{1}{2} \int_{B_1} (k_s(\operatorname{div} u)^2 + k_b(\operatorname{curl} u)^2) + \frac{1}{2\epsilon^2}(1-|u|^2)^2 dx$$

where k_s, k_b are the splay and bend constants for the liquid crystal, ϵ is the radius of the defect core and u is no longer restricted to having length 1. Due to the polarization vector field, u is given boundary conditions, i.e., $u = g$ when $|x| = 1$, $k_s \neq k_b$, and g has degree $d > 0$. For each ϵ , a minimizing vector field u_ϵ exists and as $\epsilon \rightarrow 0, u_\epsilon \rightarrow u^*$. u^* has d degree 1 singularities, and near a singularity, a , u^* behaves locally as

$$u^* = \alpha_a \frac{x - a}{|x - a|}$$

where $\alpha_a = \pm 1$ for $k_s < k_b$ and $\alpha_a = \pm i$ for $k_b < k_s$ [4].

The purpose of this project is to develop a spectral-Galerkin numerical method to solve the Euler-Lagrange equations for E_ϵ , when ϵ is small, so as to capture the experimental observations and analytical results described above. Many numerical methods deal with the case $k_s = k_b$, resulting in the Allen-Cahn equation. Our method will also simulate the case $k_s \neq k_b$ [5, 6]. We develop a gradient flow stabilized scheme to solve the Euler-Lagrange equations and let the solu-

tions stabilize to an equilibrium state. This is done due to the non-linear terms in the equations. We discretize the Euler-Lagrange equation as a first-order semi-implicit stabilized scheme. The equation is then converted into a polar geometry representation. With this representation we can approximate the solution with a Fourier expansion in the angle variable using the FFT and then approximate the Fourier coefficients using Chebyshev polynomials in the radius variable, giving the form of the approximation

$$u_{N,M} = \sum_{n=0}^N \sum_{|m|=0}^{\frac{M}{2}} (\hat{u}_{n,m}) T_n(2r-1) e^{im\theta}$$

This scheme has been shown to be unconditionally stable. Using MATLAB R2012a version 7.14.0.739, we tested the scheme with various boundary conditions having degree one and two. Figure 23 plots the minimum vector field orientation u_ϵ , given the values of k_s, k_b and the boundary data g . We see that in the case $k_s < k_b$, the vector field is nearly radial near the origin. When $k_b < k_s$, the vector field is nearly tangential near origin. This follows what was shown analytically. The plot in the case $k_s < k_b$ follows what was seen experimentally as well. In the case where $k_s < k_b$ and the vector field is tangential at the boundary, either clockwise or counterclockwise, the stable vector field is a simple spiral.

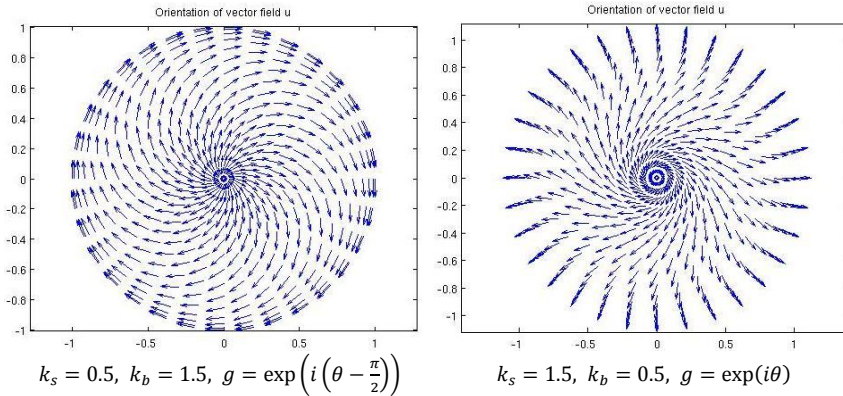


Figure 23. Stable vector fields to the free energy.

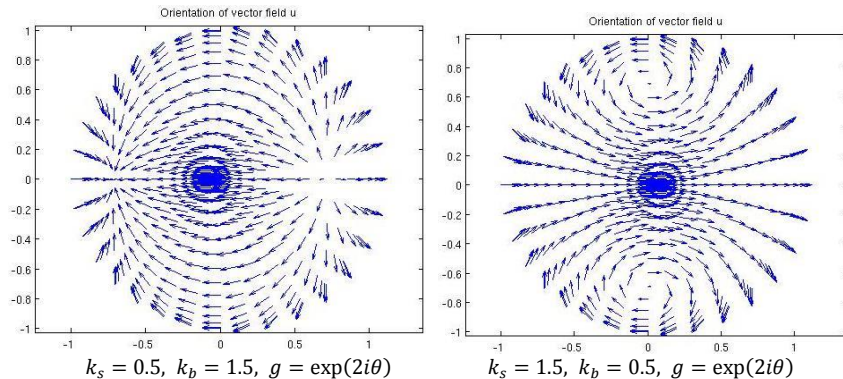


Figure 22. Stable vector fields to the free energy.

In the case of degree two boundary conditions, $g = e^{2i\theta}$, the simulations suggest uniqueness of the location for the two degree one vortices. They seem to migrate to the real axis in the case $k_s < k_b$ and to the imaginary axis in the case $k_b < k_s$, lying symmetrically about the origin, as depicted in Figure 22. This result is independent of where the initial vortices were located or whether the vortices are degree 1 or 2. Further analysis of this result needs to be done, in terms of analyzing the energy in a renormalized state, expressed in terms of the vortices, boundary data, and the vector field in the domain.

Lee, Konovalov, and Meyer [3] note that the size of the island also affects the transformation of the vector field. If the island is of small size, i.e. small radius, then the pure

bend patterns rarely transform to a simple spiral. This would be a test that could be done on the simulation to determine if we obtain similar results.

- [1] J.-B. Lee, R. A. Pelcovits, and R. B. Meyer, Role of Electrostatics in the Texture of Islands in Free-standing Ferroelectric Liquid Crystals, *Physical Review E* **75** (2007), 051701.
- [2] R. B. Meyer, L. Liébert, L. Strzelecki and P. Keller, Ferroelectric Liquid Crystals, *Le Journal de Physique Lettres* **36:3** (1975), L69-L71.
- [3] J.-B. Lee, D. Konovalov, and R. B. Meyer, Textural Transformations in Islands on Free Standing Smectic-C* Liquid Crystal Films, *Physical Review E* **73** (2006), 051705.
- [4] S. Colbert-Kelly and D. Phillips, Analysis of a Ginzburg-Landau Type Energy Model for Smectic C* Liquid Crystals with Defects, *Annales de l'Institut Henri Poincaré (C) Non Linear Analysis* **30:6** (2013), 1009-1026.
- [5] J. Shen, Efficient Spectral-Galerkin Methods III: Polar and Cylindrical Geometries, *SIAM Journal on Scientific Computing* **18:6** (199), 1583-1604.
- [6] J. Shen and X. Yang, Numerical Approximations of Allen-Cahn and Cahn-Hilliard Equations, *Discrete and Continuous Dynamical Systems. Series A* **28:4** (2010), 1669-1691.

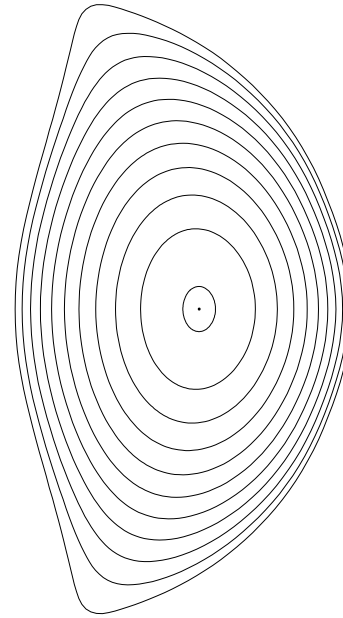


Figure 24. Magnetic flux surfaces in a three-dimensional model of the DIII-D tokamak computed by using the NSTAB equilibrium code [1]. A cross-section of the toroidal geometry is shown, with the axis of symmetry to the left of the surfaces.

Modeling Magnetic Fusion

Geoffrey McFadden

Antoine Cerfon (New York University)

A potential source of commercial energy is based on the confinement of hot plasma of hydrogen isotopes by a strong magnetic field in a toroidal geometry so the ions fuse to form helium and release energetic neutrons. A number of computational methods to model magnetic fusion devices have been developed by researchers at New York University (NYU) and elsewhere to allow effective numerical simulations of the most essential features of modern tokamak and stellarator experiments. G. McFadden and colleagues at NYU are currently participating in a benchmarking exercise to compare the simulation results produced by a number of codes that are in use by the fusion community. The benchmark is based on the DIII-D tokamak experiment at General Atomics in San Diego, California. The NSTAB equilibrium and stability code developed by Paul Garabedian and Mark Taylor at NYU [1] uses a variational formulation of the equations of magneto-hydrodynamics to compute plasma equilibria that exhibit a family of nested flux surfaces that enable plasma containment [2]. A typical NSTAB calculation is shown in Figure 24, illustrating a cross-section of the axisymmetric DIII-D geometry. The benchmarking exercise is being organized by research-

ers at the Princeton Plasma Physics Laboratory and Oak Ridge National Laboratory.

- [1] M. Taylor, A High Performance Spectral Code for Non-linear MHD Stability, *Journal of Computational Physics* **110** (1994), 407-418.
- [2] P. R. Garabedian and G. B. McFadden, Design of the DEMO Fusion Reactor Following ITER, *Journal of Research of the National Institute of Standards and Technology* **114** (2009), 229-236.

Development of a New Solver for HVAC Simulation

Anthony Kearsley

Amanda Pertzborn (NIST EL)

Jin Wen (Drexel University)

Shokouh Pourarian (Drexel University)

Dan Veronica (NIST EL)

Buildings account for 82% of the electrical energy consumption in the US [1]. Furthermore, approximately 80% of the life cycle energy use of a building is associated with its operation rather than material and construction costs [2]. Thus, optimal building operational decisions are crucial to energy efficiency. The imminent need for buildings to interact with a smart electric grid adds new opportunities to move optimal decision making for each building into the realm of

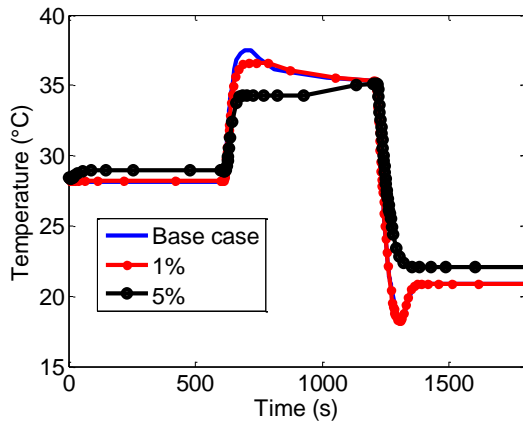


Figure 25. Temperature calculated by HVACSIM+ at one point in a basic heating coil control loop for three sets of initial guess values.

automated cyber-physical systems governed by artificial intelligence. For example, information provided to the building control system by the smart grid, such as real-time electricity pricing, can be used to make decisions about whether to use power generated by solar panels in the building itself or sell it to the utility. Development of algorithms needed to provide this intelligence requires a robust simulation testbed.

HVACSIM+, the current simulation test bed, was developed at NIST in the 1980s for the simulation of heating, ventilating, and air conditioning (HVAC) systems [3]. A specialized solver was developed for HVACSIM+ at NIST. At the time this was an advanced program, but now the limitations of HVACSIM+ are apparent: the size of the problems that can be solved is limited, it is too sensitive to initial guess values for the state of the system, and the user must be adept at formulating the problem in order to achieve a good solution.

Two examples of the sensitivity of HVACSIM+ to the initial guess values are shown in Figure 25 and Figure 26, which are based on examples taken from [4]. The model that produced Figure 25 includes a heating coil, controller, several valves, and lengths of pipe; this is a very simple model. The temperature at one point in the pipe over time is shown in the figure. The base case is the solution suggested in [4]; the 1% case was calculated by randomly perturbing some of the initial values used in the base case between -1% and 1%; the 5% case was calculated similarly. When the perturbation is only 1%, the solution changes only slightly, but when the perturbation increases to 5%, the solution changes noticeably.

Figure 26 was generated by a system including a single zone (for example, a room in a building) supplied with conditioned air by an air handler that includes a cooling coil. It is a relatively simple model as compared to what exists in an actual building. The base case was calculated following the steps described

in [4] to generate a good set of guess values. The 1% line was calculated using guess values generated by randomly perturbing the initial conditions for the base case by -1% or +1%. This small perturbation in the guess values caused the solution to diverge within the first 3 seconds of the simulation. A tool that is this sensitive to guess values that are by their nature uncertain has limited utility for the problems we envision needing to model.

Dr. J. Wen and S. Pourarian at Drexel University have been investigating the causes of this instability as part of a grant [5]. A. Kearsley has been working closely with them to develop a new, more stable solver based on the Levenberg-Marquardt method. A. Pertzborn and D. Veronica have been working to integrate this new solver into the existing program for testing.

Additional work remains to update HVACSIM+ and turn it into a tool that can be applied to the effort to fully integrate embedded intelligence with smart grid in commercial buildings. This effort requires a solver that is not only robust and stable, but is also capable of enforcing constraints to maintain the solution in a physically realistic space, handle large scale models, and reformulate a poorly designed problem.

- [1] Buildings Energy Data Book, US Department of Energy, Table 6.1.1¹², downloaded 12/6/2013.
- [2] *Transforming the Market: Energy Efficiency in Buildings*¹³, World Business Council for Sustainable Development.
- [3] D. Clark, HVACSIM+ Building Systems and Equipment Simulation Program Reference Manual, National Bureau of Standards, NBSIR 84-2996, 1984.
- [4] D. Clark and W. May, HVACSIM+ Building Systems and Equipment Simulation Program – Users Guide, National Bureau of Standards, NBSIR 85-3243, 1985.

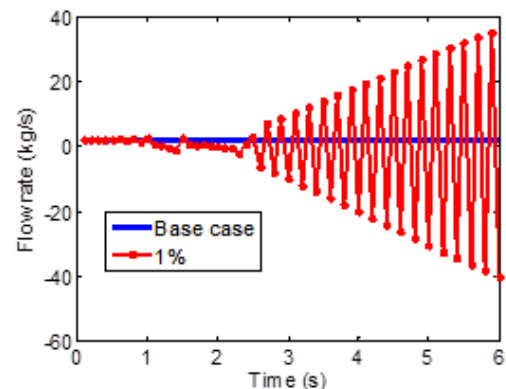


Figure 26. Flow rate calculated by HVACSIM+ for a single zone air handler with cooling coil for two sets of initial guess values.

¹² <http://buildingsdatabook.eren.doe.gov/TableView.aspx?table=6.1.1>

¹³ <http://www.wbcsd.org/Pages/EDocument/EDocumentDetails.aspx?ID=11006>

- [5] NIST Grant, Number 60NANB10D243, Tools for Evaluating Fault Detection and Diagnostic Methods for HVAC Secondary Systems of a Net Zero Building.

Sustainable Design of Reinforced Concrete Structures

Florian A. Potra
Dong Hun Yeo (NIST EL)
Emil Simiu (NIST EL)

Traditionally, the objective of structural engineering has been to achieve construction that is safe and disaster-resilient on the one hand and economical on the other. It is only recently that the scope of structural engineering has been expanded to include sustainability. According to studies conducted by the Organization for Economic Cooperation and Development (OECD), the residential and commercial building sectors are responsible for approximately 30% of primary energy consumed and of greenhouse gas emissions in OECD countries.

The contribution of reinforced concrete construction to embodied energy is significant, and modern structural design methods can help to achieve important reduction of this contribution. In spite of the use of additives such as fly ash, reinforced concrete structures, which are large consumers of cement, are responsible for a sizable proportion of worldwide carbon emissions. These emissions can be reduced significantly by using optimization techniques to devise a more efficient use of both concrete and steel. Modern optimization tools now make it possible to perform large volumes of calculations applicable to a wide variety of structural engineering problems.

This project presents an optimization approach developed with a view to allowing decision-makers to balance sustainability and economic objectives. To illustrate this approach a reinforced concrete frame under gravity and lateral loads was considered. The optimization with respect to the CO₂ footprint results in an increase in the relative amount of steel within the members' cross sections; however, the requisite ductility is assured via constraints specified in the optimization process. The reduction of the footprint achieved by optimizing the design to obtain minimum carbon emissions, as opposed to optimizing the design to achieve minimum cost, is of the order of 5% to 15%, depending upon the parameter values being assumed.

In addition, an investigation was performed into the effects of concrete compression strength on the optimization effectiveness. As the concrete strength increases, the difference between the costs of the cost-optimized and the footprint-optimized frames decreases, while the difference between the CO₂ footprints of

the cost-optimized and the CO₂-optimized frames increases. Thus, for higher strength concrete, the optimization is very effective. The initial results of this project are contained in [1].

The reduction can be smaller for low-structures and other structures with predominantly tension-controlled members. However, for structures whose members predominantly experience large compressive forces, such as high-rise buildings, the reduction may be more significant. This may also be true of certain pre-tensioned or post-tensioned concrete members. Additional research aimed at ascertaining the extent to which this is the case is warranted. Although footprint-optimized reinforced steel construction is slightly more expensive, this situation may change in the future.

Large and significant segments of American industry (e.g., Exxon, Shell, General Electric, and many others) are now accepting and including into their plans the concept of adding carbon emissions taxation to their business expenses. Including such taxes in the total construction costs makes it possible to optimize construction from the point of view of both cost and emissions. It is anticipated that the approach developed in this project will be incorporated into engineering practice via manuals of practice, standards and codes, and contribute significantly to the reduction of global carbon emissions and to a greener economy. Future research will continue with a view to rendering the approach developed so far increasingly practical and user-friendly, and attempting to incorporate it in common "green structural engineering" practice.

- [1] D. Yeo and F. A. Potra, Sustainable Design of Reinforced Concrete Structures through CO₂ Emission Optimization, Special Issue on "Sustainable Building Structures," *Journal of Structural Engineering-ASCE*, to appear.

Modeling with Uncertainty Estimation of a Thickness-Shear MEMS Resonator

Jeffrey T. Fong
Ward L. Johnson (NIST MML)
Pavel Kabos (NIST PML)
T. Mitchell Wallis (NIST PML)
Li Ma (NIST MML)
N. Alan Heckert (NIST ITL)
James J. Filliben (NIST ITL)
Pedro V. Marcal (MPACT Corp)

Johnson, et al. have recently conducted experiments at the NIST Boulder laboratory on excitation and detection of thickness-shear modes of vibration in a micro-electro-mechanical system (MEMS) resonator due to a Lorentz force produced by a current in a thin-film

waveguide in the presence of a static magnetic field. The experiments produced two results of interest, namely, (1) a vibrationally trapped thickness-shear MEMS device with Lorentz force transduction was shown to be experimentally feasible, and (2) measurable signals were not detected in the fabricated devices for acoustic resonances. The second result was disappointing, because the investigators were looking for resonances that offer the potential of providing ultra-high resolution for sensing gas and liquid-borne molecules in health care, environmental, water quality, homeland security, and defense.

An earlier attempt by Heyliger, Flannery and Johnson to estimate the first thickness-shear mode resonance frequency using a two-dimensional finite-element model and a series of ad hoc simplifying assumptions resulted in a prediction of 412 MHz [2]. However, no such measurement evidence was found in subsequent experiments [1].

The goal of this finite element modeling project is to develop a fully three-dimensional finite element model using two commercially-available general purpose software packages, ABAQUS and COMSOL, for a variety of device designs to answer three questions: (a) Why did the prediction of the earlier finite element model fail in experiments? (b) What changes in device design are likely to yield an experimentally verifiable prediction? (c) How does simulation uncertainty match the uncertainty in experiments?

- [1] W. L. Johnson, T. M. Wallis, P. Kabos, E. Rocas, E. Collado, L.-A. Liew, J.-Y. Ha, A. V. Davydov, A. Plankis and P. Y. Heyliger, A Thickness-shear MEMS Resonator Employing Electromechanical Transduction through a Coplanar Waveguide.
- [2] P. Y. Heyliger, C. M. Flannery and W. L. Johnson, *Nanotechnology* **19** (2008), 145707.

Using Quadratic Functions over Lines in Evolutionary Optimization

Anthony J. Kearsley
Ismet Sahin (University of Maryland)

Population-based metaheuristic optimization algorithms aim to find an extremum of a given function defined on a region of interest. The ease with which they can be implemented and applied to problems has resulted in an increase in their use and development [1, 2]. They are often employed when the cost function does not have derivative information (gradient or Hessian) readily available, perhaps due to its complexity, discontinuity, or nonnumeric structure. While other approaches exist for these types of problems such as direct search methods [3] or simulated annealing methods [4], this project focuses on a population set-based

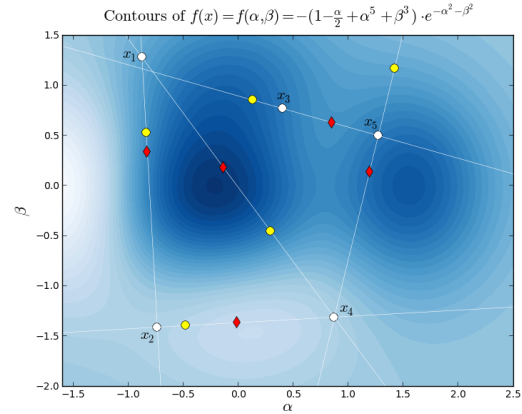


Figure 27. Contours of two dimensional cost function $f(x)$ specified in the title of the plot and five randomly selected lines. Three points are chosen over each line and a quadratic model is fit to these points. The extrema of these models are indicated by the red diamond markers. Two quadratics over the lines passing through (x_3, x_5) and (x_2, x_4) are concave for which we propose new schemes to produce mutated points in this project. Other three quadratic models are convex and their minimizers are used as mutated points for corresponding lines.

algorithm. Population-based algorithms create an initial generation of vectors where each vector is an approximation to the minimizer of the given function, and then apply evolutionary operations in order to produce new generations with improved approximations. The mutation and crossover evolutionary operations produce variations in the generation, and the selection operation chooses the variational points yielding smaller function values.

Even though many evolutionary algorithms have been proposed in the literature, their mutation operations are limited in using mathematical models that can predict the cost function surface. A recent study introduced the Random Lines (RL) algorithm, which uses quadratic function models in its mutation operation and achieves improved robustness and efficiency in finding the minimizer. However, its use of concave quadratics can be improved substantially as it now simply assigns the maximizer of the model as the mutated point.

In this project, we are motivated to develop new schemes to handle the concave cases more efficiently [6]. Figure 27 demonstrates 3 convex and 2 concave quadratic models over five randomly selected lines, where clearly minimizers of the convex models lead to the regions with smaller function values. Based on the concave models, the proposed schemes choose search directions away from the maximizers along the line. The step sizes are determined based on the distances between the points of the current generation. We demonstrate that these schemes improve robustness and efficiency substantially compared to the original RL algorithm and other evolutionary optimization algorithms. In a future work, we are planning to extend this algorithm for constrained optimization problems.

- [1] A. Torn, *Global Optimization*, Springer-Verlag, 1989.
- [2] D. G. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, Springer, 2008.
- [3] T. G. Kolda, R. M. Lewis and V. Torczon, Optimization by Direct Search: New Perspectives on Some Classical and Modern Methods, *SIAM Review* **45:3** (2003), 385-482.
- [4] S. Kirkpatrick, C. D. Gelatt and M. P. Vecchi, Optimization by Simulated Annealing, *Science* **220:4598** (1983), 671-680.
- [5] I. Sahin, Random Lines: a Novel Population Set-based Evolutionary Global Optimization Algorithm, in Genetic Programming (S. Silva, et al., eds.), *Lecture Notes in Computer Science* **6621** (2011), Springer, 97-107.
- [6] I. Sahin and A. J. Kearsley, Using Quadratic Functions over Lines in an Evolutionary Optimization Algorithm, submitted.

Separating Signal from Noise via the SVD

Bert W. Rust

Cubic splines are often used to estimate the signal in noisy measured data. One approach imposes a smoothness constraint on the equations used for calculating an interpolating spline and requires the specification of a smoothing constant to determine the amount of smoothing imposed. Another approach uses a regression spline with fewer knots than the number of observations, and requires the specification of the number and locations of those knots.

B. J. Thijsse and his colleagues [1, 2] have developed an algorithm that determines the optimal number and distribution of knots. But these results can be improved still further by solving the resulting linear regression problem by a variant of the truncated singular value decomposition method which truncates the singular vector expansion rather than the singular value distribution [3]. This method is a variant of principal components regression which does not use the singular values to choose the principal components. It produces residuals which are closer to uncorrelated white noise than are those obtained from smoothing spline approximations.

- [1] B. J. Thijsse, M. A. Hollanders and J. Hendrikse, A Practical Algorithm for Least-Squares Spline Approximation of Data Containing Noise, *Computers in Physics* **12** (1998), 93-399.
- [2] B. J. Thijsse, J. Barend and B. W. Rust, Freestyle Data Fitting and Global Temperatures, *Computing in Science & Engineering* (January/February 2008), 49-58.
- [3] B. W. Rust, Truncating the Singular Value Decomposition for Ill-Posed Problems, NISTIR 6131, July 1998.

The Metrology of Supernova Light Curves

Bert W. Rust

Katharine M. Mullen (UCLA)

We model the Type Ia supernova light curve as the superposition of three luminosity pulses: an initial pulse generated by the deposition of ^{56}Ni followed by the sub-sequent pulses generated by the radioactive decays $^{56}\text{Ni} \rightarrow ^{56}\text{Co} \rightarrow ^{56}\text{Fe}$. We assume that the two radioactive decays occur in a stable environment with density and temperature so high that the two decay rates are accelerated by the same factor. We use a three parameter Weibull probability density function to model the ^{56}Ni deposition so that the model can be written as a linear combination of the Ni-deposition pulse and the solutions to two coupled ordinary differential equations with four adjustable nonlinear parameters, specifying the time of the onset of Ni-deposition, the shape and the scale of the deposition pulse, and the acceleration factor for the two decay rates. The three linear parameters specify the energies associated with the three processes and enable the estimation of the energy/nucleon emitted by the Ni-deposition.

Fitting the model to the measured light curves for a sample of relatively nearby supernovae gave fits that explained more than 99 % of the total variance in every case. Such high fidelity to the measured data indicates that the fitted light curves may give more precise estimates of important parameters like the maximum luminosity and the time at which it occurs, the rise time to maximum luminosity, and the decline rate of the luminosity in the tail of the curve.

Such improved precision should prove very beneficial in calibrating the extragalactic distance scale and performing cosmological tests with very distant supernovae. For the small sample that has been analyzed thus far, the average of the estimates for the energy/nucleon in the Ni-deposition pulse is slightly greater than the binding energy of ^{56}Ni .

- [1] B. W. Rust, M. Leventhal and S. L. McCall, Evidence for a radioactive decay hypothesis for supernova luminosity, *Nature* **262** (1976), 118-120.
- [2] B. W. Rust and K. M. Mullen, The Metrology of Supernova Light Curves, poster, 223rd Meeting of the American Astronomical Society, Washington D.C., Jan. 8, 2014.

Sparse Low-rank Nonnegative Approximation of Interval Matrices

Dianne P. O'Leary

Yi-Kai Liu

John M. Conroy (IDA CCS)

Daniel Samarov (NIST ITL)

Data often has a simple underlying structure that is obscured by measurement error or missing values. For example, in spectroscopy, the true spectrum is a weighted sum of some dictionary spectra corresponding to the components in the sample. Similarly, in classifying a set of documents, the values in a matrix might represent the importance of each term in each document, but some values might be missing and others are quite noisy, obscuring the underlying dictionary of topics. The same problem arises in other matrix completion problems, where, for example, the preference of each customer for each product should be estimated from an incomplete set of preferences.

Each of these matrix approximation or matrix completion problems has the same structure. The idea is to approximate a given matrix \mathbf{A} , which we don't know with certainty, by a nonnegative low-rank matrix.

Previous approaches to these problems minimize the difference between the noisy measurements \mathbf{A} and the computed low-rank matrix.

Our approach is different: we assume that we are given upper and lower bounds on each entry of the true matrix. These bounds are determined from the measured values and their uncertainties. This defines an interval in which the true unknown matrix lies. We minimize the difference between the computed low-rank matrix and the closest matrix that lies within the interval. We also allow weights in measuring this difference; for example, if we have no information about a particular element of \mathbf{A} , we might set the corresponding weight to zero. As in previous approaches, we can add a penalty term to enhance sparsity in the approximation.

We developed an alternating minimization algorithm to solve this problem and tested it on problems in document classification and (simulated) spectral analysis. On data from NIST's 2004 Document Understanding Conference (DUC-04) competition, our new approach improved the performance measure known as adjusted mutual index from 0.70 to 0.82, where 1.00 indicates that all documents were classified correctly. We are extending the approach to tensor approximation.

- [1] J. Conroy, S. T. Davis, J. Kubina, Y.-K. Liu, D. P. O'Leary and J. D. Schlesinger, Multilingual Summarization: Dimensionality Reduction and a Step towards Optimal Term Coverage, in *Proceedings of the Workshop on Multilingual Multi-document Summarization (MultiLing 2013)*, Sofia, Bulgaria, August 2013, 55-63.

Advanced Manufacturing

Delivering technical support to the nation's manufacturing industries as they strive to out-innovate and out-perform the international competition has always been a top priority at NIST. This has also emerged as a major White House priority in recent years, in which NIST is playing an increasingly central role. Mathematical modeling, computational simulation, and data analytics are key enablers of emerging manufacturing technologies. This is most clearly evident in the Materials Genome Initiative, an interagency program with the goal of significantly reducing the time from discovery to commercial deployment of new materials through the use of modeling, simulation, and informatics. ACMD's role in advanced manufacturing centers on the development and assessment of modeling and simulation tools, with emphasis on uncertainty quantification, as well as support of NIST Laboratory efforts in such areas as nonmanufacturing, smart manufacturing, and materials modeling.

Rheology of Dense Suspensions

*William George
Steven Satterfield
Marc Olano
Judith Terrill
Nicos Martys (NIST EL)
Edward Garboczi (NIST EL)
Pascal Hebraud (CNRS/ESPCI, France)*

See page 59.

Micromagnetic Modeling

*Michael Donahue
Donald Porter
Robert McMichael (NIST CNST)
June Lau (NIST MML)*

<http://math.nist.gov/oommf/>

Advances in magnetic devices such as recording heads, field sensors, spin torque oscillators, and magnetic nonvolatile memory (MRAM) are dependent on an understanding of magnetization processes in magnetic materials at the nanometer level. Micromagnetics, a mathematical model used to simulate magnetic behavior, is needed to interpret measurements at this scale. ACMD is working with industrial and academic partners, as well as with colleagues in the NIST CNST, MML, and PML, to improve the state-of-the-art in micromagnetic modeling.

Michael Donahue and Donald Porter in ACMD have developed a widely used public domain computer code for doing computational micromagnetics, the Object-Oriented Micromagnetic Modeling Framework (OOMMF). OOMMF serves as an open, well-documented environment in which algorithms can be evaluated on benchmark problems. OOMMF has a modular structure that allows independent developers to contribute extensions that add to its basic functionality. OOMMF also serves as a fully functional

micromagnetic modeling system, handling both two and three-dimensional problems, with sophisticated extensible input and output mechanisms. In FY 2013 alone, the software was downloaded more than 11,000 times, and use of OOMMF was acknowledged in some 150 peer-reviewed journal articles. OOMMF has become an invaluable tool in the magnetics research community.

Key new developments over the last year include:

- a) Derivation of new equations for cell-to-cell demagnetization tensor values that produce fourth order precision with respect to cell edge length.
- b) Enhancement of robustness against data loss with pre-loading of code that manages error handling and improved logging of data archiving operations.
- c) Creation of a new application to manage and manipulate tables of output quantities.

Ongoing work includes collaboration with the University of California, San Diego on porting OOMMF calculations to massively parallel graphical processing units (GPUs) with Materials Genome Initiative support.

OOMMF is part of a larger activity, the Micromagnetic Modeling Activity Group (muMAG), formed to address fundamental issues in micromagnetic modeling through two activities: the development of public domain reference software, and the definition and dissemination of standard problems for testing modeling software. ACMD staff members are involved in development of the standard problem suite as well. Ongoing work includes the development of new OOMMF capabilities and data processing utilities to facilitate the collection and reporting of points of comparison defined in standard problems.

In addition to the continuing development of OOMMF, the project also does collaborative research using OOMMF. Recent work has applied OOMMF to the investigation of the structure and periodicity of cross-tie walls in thin magnetic strips. A new contributed extension from Laboratoire de Physique des Solides (Universite Paris Sud) adds calculation of the Dzyaloshinskii-Moriya interaction (DMI) to OOMMF

simulations, enabling the study of skyrmions, a subject of widespread current interest. The availability of the OOMMF source played a key role in a new understanding of the effect of boundary conditions on the DMI.

The ACMD micromagnetic project produced two conference presentations this past year.

- [1] M. J. Donahue, "Structure and Periodicity of Cross-tie Walls in Thin Magnetic Strips," 12th Joint MMM/Intermag Conference, Chicago, IL, Jan. 16, 2013.
- [2] D. G. Porter, "Scaling Tcl Data Structures," 20th Annual Tcl/Tk Conference, New Orleans, LA, Sept. 26, 2013.

OOF: Finite Element Modeling of Material Microstructures

Stephen A. Langer

Andrew C.E. Reid (MML)

Gunay Doğan (Theiss Research)

Faical Yannick Palingwende Congo (ISIMA)

<http://www.ctcms.nist.gov/oof/>

The Object Oriented Finite Elements (OOF) Project, a collaboration between ACMD and MML, is developing software tools for analyzing real material microstructure. The microstructure of a material is the (usually) complex ensemble of polycrystalline grains, second phases, cracks, pores, and other features occurring on length scales large compared to atomic sizes. The goal of OOF is to use data from a micrograph of a real or simulated material to compute the macroscopic behavior of the material via finite element analysis. OOF is intended to be a general tool, applicable to a wide variety of microstructures in a wide variety of physical situations.

The OOF development team consists of two NIST staff, Steve Langer and Andrew Reid, and two guest researchers, Gunay Doğan and Yannick Congo. Langer works on OOF full time, and Reid splits his time between OOF and other duties in MML. Doğan works on OOF and shape metrology. Congo works full time on the OOF test suite and comes to NIST from Burkina Faso, by way of ISIMA and Université Blaise-Pascal in France.

The currently available version of OOF is OOF2, which solves two dimensional time-dependent problems based on two dimensional micrographs. Version 2.1.8 was released this year, but since it only fixed a few rarely encountered bugs and added a couple of specialized features requested by users, it was released quietly, without an official announcement. The specialized features were modifications to the build script to allow the program to be run on some uncommon computer configurations and the addition of a "Pause"

button to control prerecorded demonstrations of the software, making it more useful as a pedagogical tool. As a diagnostic test, at one point OOF2 was ported to the popular Raspberry Pi credit-card-sized computer. This highly resource-constrained environment revealed a bug in the allocation of memory at start-up time, which has now been fixed.

OOF2 continues to be used in the materials science community. The source code was downloaded more than 1 100 times during FY 2013. The program can also be run on-line at nanoHUB¹⁴, where it was used in more than 2 500 sessions this year.

A large part of the development effort this year went toward OOF3D, the soon to be released three dimensional version of OOF. OOF3D will read three dimensional microstructural datasets from experiments or simulations and perform fully three dimensional computations on them.

Work has been centered on the test suites, the development of which has revealed numerous bugs and missing features. The goal is to ensure that before the first version of OOF3D is released, all of its critical features are implemented and tested. It must be able to solve a full problem, from microstructure to post-processing analysis, and must be able to do so in a manner that is not too laborious for the user. Some features can be copied directly from OOF2 (e.g., command and control infrastructure), some require various degrees of modification from their OOF2 versions (e.g., addition of groups of faces to the existing element, segment, and node groups), and some are completely new (e.g., detecting whether a set of element faces forms an orientable surface on which boundary conditions can be applied).

An interesting discovery this year was that the OOF3D GUI (graphical user interface) tests were sensitive to the choice of a window theme on some computers. A test script recorded on one computer with one windowing system would fail when replayed on a different computer. Changing the GUI theme would change the size of the labels on GUI buttons and other widgets, which would slightly change the space allocated for the OOF3D graphics canvas, which would slightly change the position of objects drawn in the canvas, which would drastically change the interpretation of mouse clicks on the canvas. The solution was to add information about the canvas size to the GUI log script, in addition to information about window size changes.

At the end of FY 2013 only two major features still needed to be added to OOF3D before it could be released: Neumann boundary conditions and post-processing of output. Neumann boundary conditions can be implemented in the same general way as they are in OOF2, but require methods for integrating over

¹⁴ <http://www.nanohub.org/>

surfaces and specifying locations on surfaces that are new to 3D. (They are not conceptually difficult, but require care in their implementation to ensure correctness, flexibility, and maintainability.) Post-processing likewise will mostly involve copying code from OOF2, but must be extended to handle different ways of specifying the domain of the post-processing commands. For example, in 3D there are both linear and planar cross sections, and it's not possible to choose the left or right side of a linear cross section the way it is in 2D.

Other development efforts will benefit both OOF2 and OOF3D. Andrew Reid completed evaluation of a constitutive rule for solid-state deformation scenarios where the system remains permanently deformed after the applied loads are removed. Once implemented in OOF, this will allow it to contribute to studies of metal forming of interest to the Materials Genome Initiative.

Image segmentation, namely, identification of phases or regions and their boundaries in given microstructure images, is a critical step in both OOF2 and OOF3D. Once the distinct regions forming the microstructure have been identified, users can generate computational meshes conforming to the regions for different materials and simulate various physics using these meshes. In this fiscal year, Gunay Doğan worked to improve and extend previously developed segmentation models to be able to handle more diverse imaging scenarios in an efficient and robust manner. The main focus of this work was region-based and edge-based segmentation models. To ensure consistent and reliable performance in difficult situations, such as low-contrast or high-noise images, he implemented various improvements to the underlying shape optimization algorithms. The details of this work are given in the section for Computational Tools for Shape Measurement and Analysis (see page 39).

Future goals for the OOF project include:

- Merging the OOF2 and OOF3D code bases so that future improvements can be made to both programs simultaneously. A lot of code is already shared between the two, but many changes in OOF2 have not been made in OOF3D and vice versa.
- Providing an easily extensible platform for two and three dimensional plasticity calculations.
- Providing advanced image segmentation tools within OOF2 and OOF3D.
- Parallelizing the time-critical code, especially in OOF3D.

Solving the Diffusion Equation in Microstructures

Javier Bernal

Nicos Martys (NIST EL)

Scott Jones (NIST EL)

Software is being implemented for solving the diffusion equation in microstructures that represent cracked concrete. This software will be utilized to predict the influence of cracks on the service life of concrete. The microstructures will be meshed using a Voronoi construct in order to provide a realistic representation of the crack/pore interface. The Voronoi construct should allow for the development of a multiscale representation of the cracked microstructure in a way that will improve computational efficiency and accuracy.

Moving Grain Boundary Grooves under Stress

Geoffrey McFadden

William Boettinger (NIST MML)

Robert Sekerka (Carnegie Mellon University)

Grain boundaries are the interfaces that separate individual grains of a crystalline material that have different orientations of the crystal axes in each grain. Grain growth occurs by grain boundary motion, which is subject to energetic driving forces from effects such as surface tension, which tends to minimize net surface energy, and elastic forces, which tend to minimize strain energy. In thin films of polycrystalline material, the presence of lateral compressive or tensile stresses can cause migration of a grain boundary with an associated deformation of the nearby solid-vapor interface at the film surface. These features are commonly observed in thin films under compression, and have been conjectured to lead to the formation of crystalline “whiskers” that can bridge gaps between electronic components and lead to electrical failure.

Models of grain boundary motion when the slope of the solid-vapor interface is small have been developed by Mullins and co-workers in a variety of contexts [1, 2]. In work completed this fiscal year we have extended the model to finite slopes. In a sample with two-dimensional geometry this results in a system of nonlinear fourth-order ordinary differential equations in a coordinate system that moves with the velocity of the grain boundary. We have computed finite-amplitude solutions to the governing equations that extend the small-amplitude theory, and have also improved the model in [2] by formulating conditions

that maintain the equality of chemical potential at the trijunction [3].

- [1] W. W. Mullins, The Effect of Thermal Grooving on Grain Boundary Motion, *Acta Metallurgica* **6** (1958), 414-427.
- [2] F. Y. Genin, Effect of stress on grain boundary motion in thin films, *Journal of Applied Physics* **77** (1995) 5130-5137.
- [3] R. F. Sekerka, W. J. Boettinger and G. B. McFadden, Surface Morphologies due to Grooves at Moving Grain Boundaries Having Stress-Driven Fluxes, *Acta Materialia* **61** (2013) 7216-7226.

Morphological Stability

Geoffrey McFadden

Sam Coriell (NIST MML)

Robert Sekerka (Carnegie Mellon University)

In the production of metallic or semiconductor alloy crystals it is usually desirable that the concentration distributions be spatially uniform, as heterogeneous alloy concentrations can seriously degrade material performance. Crystal growth is therefore usually performed under highly controlled conditions to achieve high levels of homogeneity. A common technique is Bridgman growth, in which the crystal is grown “directionally” in a one-dimensional temperature gradient that in principle produces a planar interface separating the cooler growing solid phase from the hotter molten phase. If the solutes are uniformly distributed in the melt at the solid-liquid interface, the resulting crystal has the desired levels of homogeneity.

In practice the system can be subject to instabilities that produce non-planar interfaces, which result in associated non-uniform concentration distributions in the growing crystal. The study of such instabilities has therefore been an area of fundamental importance in materials processing, dating back to the early days of the development of semiconductor technology. A landmark contribution to the field was the theoretical work published in 1964 [1] by W. W. Mullins and R. F. Sekerka that has become known as the theory of *morphological stability*. They explained how the temperature and concentration gradients at the solid-liquid interface can lead to “constitutional supercooling” instabilities that are analogous to the instabilities commonly observed when freezing a pure material that has been cooled to temperatures below the material’s melting point. A large literature has been since produced on the theory of morphological stability and on related aspects of this phenomenon during materials processing. In particular, this has been an important area of research at NIST, where R. F. Sekerka has been an active consultant since the 1970’s.

A 72 page review article on morphological stability was written by S. R. Coriell and G. McFadden in 1993 [2] for the three volume *Handbook of Crystal Growth*. The article covers the technical aspects of the theory in some detail, including the discussion of a number of extensions of the theory, with 242 references to the literature.

That article has been well received, but because of the continuing activity in the field over the ensuing twenty years it is now somewhat dated due to the appearance of subsequent work. A second edition of the handbook is now in preparation, and a revised version of this review article has been written by R. F. Sekerka, S. R. Coriell, and G. B. McFadden [3]. This article is intended to include recent references to the subject, and to present the theory at a level that is accessible to the non-expert. The article has been submitted to the handbook editor, and will appear in the second edition of the Handbook.

- [1] W.W. Mullins and R.F. Sekerka, Stability of a planar interface during solidification of a dilute binary alloy, *Journal of Applied Physics* **35** (1964) 444-451.
- [2] S. R. Coriell and G. B. McFadden, Morphological Stability, Chapter 12 in *Handbook of Crystal Growth*, Volume 1b. Transport and Stability, (D. T. J. Hurle, ed.), North-Holland, Amsterdam, 1993, 785-857.
- [3] R. F. Sekerka, S. R. Coriell, and G. B. McFadden, Morphological Stability, in *Handbook of Crystal Growth*, 2nd edition (T. Nishinaga, ed.), North-Holland, Amsterdam, to appear.

Inverse Method for Estimating Shear Stress in Machining

Timothy Burns

Steven Mates (NIST MML)

Richard Rhorer (NIST EL)

Eric Whitenon (NIST EL)

Debasis Basak (Orbital Sciences Corporation)

A major reason for the lack of predictive capability of finite-element based machining models is the lack of good constitutive response models for the flow stress in the chip material during a rapid material removal process. The conditions of rapid and very large shearing deformation, heating rates as high as one million degrees C per second, resulting in enormous temperature gradients, and peak temperatures on the order of 1000 °C in the thin primary shear zone where cutting takes place, and in the secondary shear zone, the thin boundary layer region where the work material continues to deform as it moves along the cutting edge of the tool (see Figure 28), are much more extreme than the conditions that most current materials testing laboratories can reproduce, control, and measure accurately.

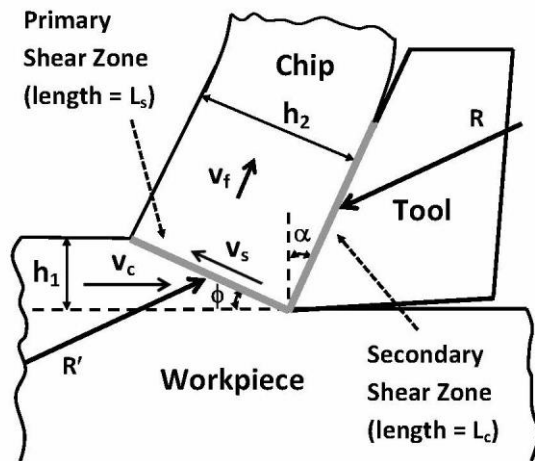


Figure 28. Schematic of orthogonal cutting, showing primary and secondary shear planes; shear angle ϕ ; rake angle α ; force between tool face and chip R ; force between workpiece and chip along primary shear plane R' ; cutting velocity v_c ; shearing velocity v_s ; and chip velocity v_f .

We have developed an inverse method for estimating the flow stress in the chip in the region of chip-tool contact along the rake face of the tool, during orthogonal machining. The method gives a formula for the peak stress in the chip on the rake face, that is based on an estimate of the temperature of the work material as it exits the primary shear zone, an experimental measurement of the peak temperature in the work material along the tool-chip interface, and a two-zone empirically based contact model for friction along this interface. We have also shown how the method can be generalized to provide an estimate of the stress in the chip on the rake face, and in the primary shear zone, given experimentally determined cutting force measurements and a discrete set of steady-state temperature measurements along the cutting edge of the tool, even when no friction model is specified. In the latter case, the inverse problem of determining the shear stress in the chip along the tool rake face can be interpreted as a problem requiring the deconvolution and unfolding of a Volterra integral equation of the first kind [1].

We are in the process of applying our method to estimate the flow stress during high-speed machining of the titanium alloy Ti-6Al-4V, using cutting force and temperature data that have been obtained using the new instrumented transparent yttrium aluminum garnet (YAG) tool that has recently been developed by Menon and Madhavan [2]. Ti-6Al-4V is a material that is widely used in aircraft manufacture. It is difficult to machine, because it has a low heat capacity and heats up very rapidly, leading to tool breakage, shear localized chips, and other difficulties. The goal of our work is to provide improved machining process simulation capabilities.

- [1] T. J. Burns, S. P. Mates, R. L. Rhorer, E. P. Whitenon, and D. Basak. Inverse method for estimating shear stress in machining, in review.
- [2] T. Menon and V. Madhavan. High accuracy full-field infrared thermography of the chip-tool interface through transparent cutting tools while machining Ti-6Al-4V, in review.

Model Selection for Fracture and Fatigue Failure Data of Engineering Materials

Jeffrey T. Fong

N. Alan Heckert (NIST ITL)

James J. Filliben (NIST ITL)

Stephen W. Freiman (NIST MML)

Pedro V. Marcal (MPACT Corporation)

One of the most hotly-debated questions in engineering design and failure analysis is how best to fit a set of fracture and fatigue failure data. In an ASTM recommended standard practice for advanced ceramic materials [1], it is assumed that a two-parameter Weibull distribution with a zero location parameter will “best” fit the data. This leads to a physically unrealistic and highly conservative assumption that among all possible samples of an engineering material, one will fail a uniaxial tensile strength test at zero load. Also unduly conservative will be the so-called A- and B-basis design allowables for failure strength at 95% confidence when the location parameter is assumed to be zero at origin of the axis.

In this work, we take a brute-force and somewhat “exhaustive” approach by developing a validation tool to answer the question how “best” a given set of univariate strength data will fit a distribution without assuming a zero location parameter. We select two methods of parameter estimation and apply four criteria of goodness-of-fit to more than 60 commonly-known distributions to see how they rank among themselves according to each of the eight combinations of parameter-estimation method plus goodness-of-fit criterion. We then develop a composite index for the eight individual rankings and order all 60+ distributions in a list for selecting the most “appropriate” distribution for the given data set.

The two parameter estimation methods are:

1. Maximum Likelihood Method [2].
2. Probability Plot Correlation Coefficient Method

The four goodness-of-fit criteria are:

1. Kolmogorov-Smirnov Criterion [4]
2. Anderson-Darling Criterion [5, 6]
3. Akaike-Burnham-Anderson Criterion [7, 8]

4. Probability Plot Correlation Coefficient Criterion [3]

Using the public-domain statistical analysis software DATAPLOT [9], we developed a model selection validation tool, and demonstrated its feasibility by applying it to six sets of data: a glassy material, two steels, two ceramic materials, and aluminum oxide [10]. We also wrote a PYTHON-based management code to automate the complex series of data analysis tasks including an input module linked to Excel [10].

- [1] *ASTM, Standard Practice for Reporting Uniaxial Strength Data and Estimating Weibull Distribution Parameters for Advanced Ceramics*, ASTM Designation: C 1239-07, Committee C28 on Advanced Ceramics, West Conshohocken, PA, 2008.
- [2] J. Aldrich, R. A. Fisher and the Making of Maximum Likelihood 1912–1922, *Statistical Science* **12: 3** (1997), 162–176.
- [3] J. J. Filliben, The Probability Plot Correlation Coefficient Test for Normality, *Technometrics* **17:1** (1975), 111-117.
- [4] F. J. Massey, Jr., The Kolmogorov-Smirnov Test for Goodness of Fit, *Journal of the American Statistical Association* **46** (1951), 68-78.
- [5] T. W. Anderson and D. A. Darling, Asymptotic Theory of Certain ‘Goodness of Fit’ Criteria based on Stochastic Processes, *Annals of Mathematical Statistics* **23** (1952), 193-212.
- [6] T. W. Anderson and D. A. Darling, A Test of Goodness of Fit, *Journal of the American Statistical Association* **49** (1954), 765-769.
- [7] H. Akaike, A New Look at the Statistical Model Identification, *IEEE Transactions on Automatic Control* **19:6** (1974), 716-723.
- [8] K. P. Burnham and D. R. Anderson, Multimodel Inference: Understanding AIC and BIC in Model Selection, *Sociological Methods and Research* **33** (2004), 261-304.
- [9] J. J. Filliben and N. A. Heckert, *Dataplot: A Statistical Data Analysis Software System*¹⁵, NIST, Gaithersburg, MD, 2002.
- [10] J. T. Fong, A. N. Heckert, J. J. Filliben, P. V. Marcal, and S. W. Freiman, A Multi-Distribution and Multi-Goodness-of-Fit-Criterion Method of Finding the Most Probable Underlying Distribution for a Given Set of Univariate Data, in preparation.

Structural Design Allowables for Composites

Jeffrey T. Fong

N. Alan Heckert (NIST ITL)

James J. Filliben (NIST ITL)

J. D. Daniel Melo (Federal University of Rio Grande do Norte, Brazil)

Carlos A. Cimini, Jr. (Federal University of Minas Gerais, Brazil)

Stephen W. Tsai (Stanford University)

The purpose of this work is to evaluate a 2002 study [1] on a comparison of 12 composites failure theories with 14 experiments using only point estimates of mean values. We conclude that “the designer wishing to estimate the ultimate failure strength of a multi-directional laminate can at best hope for accuracy of +/- 50 % in the majority of cases.”

In our work, we propose an alternative approach of testing theories against experiments by using interval estimates and the associated concept of uncertainty. For each given failure criterion, we first apply the classical law of error propagation [2] to estimating the uncertainty of the failure stress (and/or strain) as a function of the uncertainties of the material parameters. We then apply the concepts of “coverage” and “tolerance limits” to estimate the A- and B-basis allowables [3, 4] for multi-directional laminate design against failure. To illustrate our uncertainty-based approach [5], we introduce two failure criteria, one uniaxial and the other bi-axial, both of which are derived from the composites failure theories of Tsai and Wu [6], Hashin [7], and Christensen [8], to obtain results that refute the 2002 study [1].

- [1] M. J. Hinton A. S. Kaddour and P. D. Soden, A Comparison of the Predictive Capabilities of Current Failure Theories for Composite Laminates, Judged Against Experimental Evidence, *Composites Science and Technology* **62** (2002), 1725-1797.
- [2] H. H. Ku, Notes on the Use of Propagation of Error Formulas, *NBS Journal of Research* **70C:4** (1966), 263-273.
- [3] *Composite Materials Handbook – Polymer Matrix Composites Guidelines for Characterization of Structural Materials*¹⁶, MIL-HDBK-17/1 Rev. F, June 2002, (Vol. 1 of 5), U.S. Department of Defense Handbook, Chapter 8 – Statistical Methods.
- [4] J. T. Fong, C. Cimini, D. Melo, J. J. Filliben and N. A. Heckert, Theoretical Failure Envelopes of Open Hole Composite Laminates with A- and B-bases Allowables Estimated from Smooth Specimen Properties, in *Proceedings of 2013 International Conference on Composites Design*, Montreal, Canada, July 2013.

¹⁵ <http://www.itl.nist.gov/div898/software/dataplot.html>

¹⁶ <http://snebulos.mit.edu/projects/reference/MIL-STD/MIL-HDBK-17-1F.pdf>

-
- [5] J. T. Fong, J. J. Filliben and N. A. Heckert, Composites Failure Criteria, Uncertainty Propagation, and Estimation of the A- and B-basis Design Allowables, in preparation.
- [6] S. W. Tsai and E. M. Wu, A General Theory of Strength for Anisotropic Materials, *Journal of Composite Materials* **5** (1971), 58-80
- [7] Z. Hashin, Failure Criteria for Unidirectional Fiber Composites, *Journal of Applied Mechanics* **47** (1980), 329-334.
- [8] R. M. Christensen, Stress Based Yield/Failure Criteria for Fiber Composites, *International Journal of Solids and Structures* **34** (1997), 529-543.

High Performance Computing and Visualization

Computational capability is advancing rapidly. This means that modeling and simulation can be done with greatly increased fidelity (e.g. higher resolution, more complex physics). However, developing large-scale parallel applications remains highly challenging, requiring expertise that application scientists rarely have. In addition, the hardware landscape is changing rapidly, and so new algorithmic techniques must constantly be developed. We are developing and applying facilities and expertise of this type for application to NIST problems. Large scale computations and laboratory experiments invariably produce large volumes of scientific data, which cannot be readily comprehended without some form of visual analysis. We are developing the infrastructure necessary for advanced visualization of scientific data, including the use of 3D immersive environments and applying this to NIST problems. One of our goals is to develop the 3D immersive environment into a true interactive measurement laboratory.

A Dynamic Computational Phantom for RF Propagation in Body Area Networks

John Hagedorn
Kamran Sayrafian
Martina Barbi
Judith Terrill

See page 96.

Rheology of Dense Suspensions

William George
Judith Terrill
Steven Satterfield
Marc Olano
Nicos Martys (NIST EL)
Edward Garboczi (NIST EL)
Pascal Hebraud (CNRS/IPCMS, Strasbourg, France)

Understanding the mechanisms of dispersion or agglomeration of particulate matter in complex fluids, such as suspensions, is of technological importance in many industries such as pharmaceuticals, coatings, and construction. These fluids are disordered systems consisting of a variety of components with disparate properties that can interact in many different ways. Modeling and predicting the flow of such systems represents a great scientific and computational challenge requiring large-scale simulations.

In collaboration with scientists in NIST's Engineering Laboratory (EL), we have developed an application, called QDPD [1] (Quaternion-based Dissipative Particle Dynamics), which is capable of performing large-scale simulations of dense suspensions. This simulator uses a modified version of the DPD technique [2] for the simulation of Newtonian fluids, and the Smoothed Particle Hydrodynamics technique (SPH) [3] for the simulation of non-

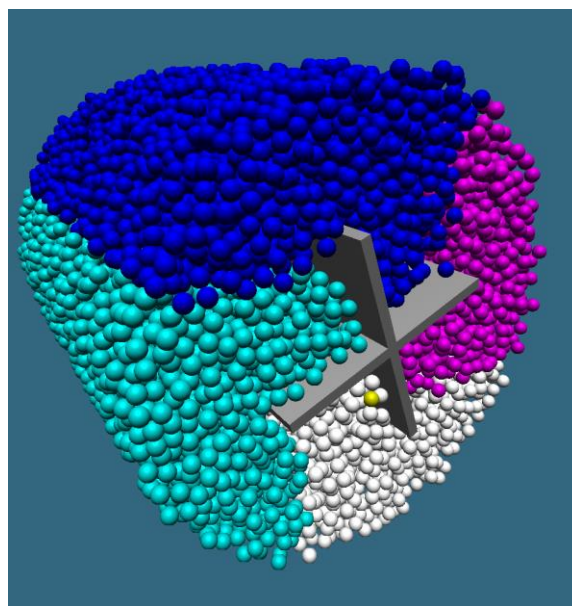


Figure 29. A snapshot from a QDPD simulation of a 4-blade rheometer with a view from the bottom of the rheometer. From this view, the blades are rotating clockwise. The suspended spheres are color-coded by their starting quadrant.

Newtonian fluids.

QDPD is highly parallel and has been shown to efficiently scale up to at least 32 000 processors when running on the DOE supercomputer Intrepid (IBM Blue Gene/P) at the Argonne National Laboratory. Our goal in this project is to advance our understanding of the flow properties of a specific material, fresh concrete, a dense suspension composed of cement, water, sand, and rocks.

We are currently using this computational approach in the development of standard reference materials (SRMs) for the calibration of vane rheometers used to measure the flow properties of fresh concrete. While concrete flow measurements, using different existing concrete rheometers, can be found to correlate, they usually do not provide results in fundamental units. This is a consequence of the

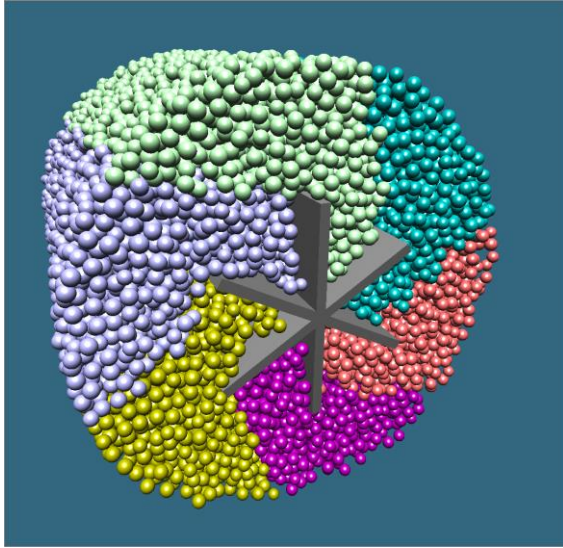


Figure 31. A snapshot from a QDPD simulation of a 6-blade rheometer with a view from the bottom of the rheometer. From this view, the blades are rotating clockwise. The suspended spheres are color-coded by their starting quadrant.

complex flow patterns that develop in the vane rheometer combined with the non-Newtonian behavior of the mortar or concrete. This results in complex local stress and strain/strain rate fields making it difficult to express measurement data in terms of fundamental rheological parameters. By modeling the flow of an SRM in a vane rheometer we are able to predict what should be measured by an experimentalist, and further, our simulations are designed to enable us to map out many details of the local flow, such as stress/strain fields in 3D, and bring insight into the vane rheometer measurement process.

Most research on suspensions has made the simplifying assumption that the matrix fluid, that is, the fluid supporting the suspended particle, is Newtonian. With the use of high-performance computing, we have been able to extend this research to include the simulation of suspensions with non-Newtonian fluid matrices, which includes most suspensions of interest to industry. One result of our studies has been to show that the viscosity versus shear rate curves for suspensions having various volume fractions can be collapsed onto a single universal curve parameterized by the properties of the underlying non-Newtonian matrix fluid [4]. This, along with other results from our studies, has advanced our basic understanding of the flow of dense suspensions [5-6].

Building on this research, we have begun using simulation in the design process for new SRMs, as described earlier, which will be used for calibrating mortar and concrete rheometers. The first such SRM will be a mortar SRM, which is expected to be released in early 2014. Our simulations of this SRM were completed in 2012-2013. The second SRM to be

developed will be a concrete SRM, for which we will begin simulations in 2014.

Along with the development of these SRMs, in 2014 we will also be extending QDPD to simulate rheometers with new blade geometries. Our simulator currently assumes that the rheometer has a simple vane design consisting of either four or six flat blades (Figure 29 and Figure 31). As we begin this study we will add to this a new double helix blade design (Figure 30), and possibly others such as a screw blade.

Novel rheometer blade designs suggested by the simulations will be constructed at NIST using additive manufacturing techniques for polymers and metals, and NIST experimental results will be compared to the simulation results.

To support this study, in June of 2013 we submitted a proposal for supercomputer time to the DOE INCITE program (Innovative and Novel Computational Impact on Theory and Experiment¹⁷). As a result of this proposal we have been awarded 40 million CPU-hours of supercomputer time for calendar year 2014 on the IBM Blue Gene/Q, Mira, at the Argonne Leadership Computing Facility. Mira is currently ranked 5th on the Top 500 list of

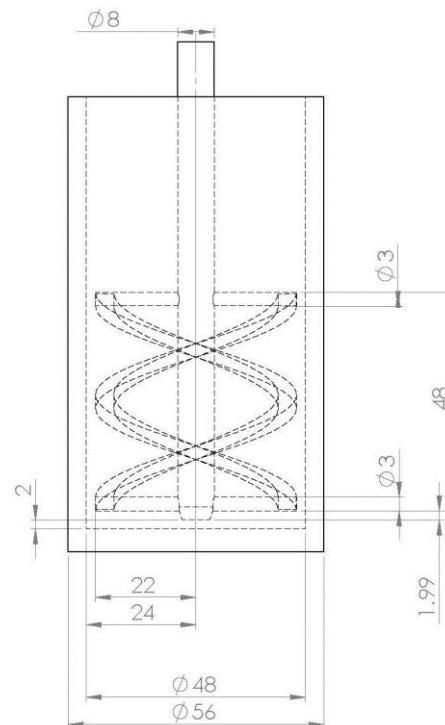


Figure 30. A design drawing for a proposed “double helix” rheometer.

¹⁷ <http://www.doeleadershipcomputing.org/>

supercomputer installations¹⁸ and will thus enable us to perform a suite of detailed simulations.

- [1] N. Martys, Study of a Dissipative Particle Dynamics Based Approach for Modeling Suspensions, *Journal of Rheology* **49:2** (2005).
- [2] P. J. Hoogerbrugge and J. M. V. A. Koelman, Simulating Microscopic Hydrodynamic Phenomena with Dissipative Particle Dynamic, *Europhysics Letters* **19** (1992), 155-160.
- [3] J. J. Monaghan, Smoothed Particle Hydrodynamics, *Reports on Progress in Physics* **68** (2005), 1703–1759.
- [4] N. Martys, M. Liard, P. Hebraud, W. George, Universal Scaling Law for the Flow of non-Newtonian Colloidal Suspensions, Society of Rheology 85th Annual Meeting, Montreal, Canada, October 2013.
- [5] N. S. Martys, M. Khalil, W. George, D. Lootens, and P. Hebraud, Stress Propagation in a Concentrated Colloidal Suspension under Shear, *The European Physical Journal E* **35:3** (2012).
- [6] P. Hebraud, D. Lootens, and N. Martys, Stress Organization in an Attractive Concentrated Colloidal Suspension under Flow, XVIth International Conference on Rheology, Lisbon, Portugal, Aug-2012.

Modeling and Visualization of Cement Paste Hydration and Microstructure Development

William George
 Steven Satterfield
 Judith Terrill
 Terence Griffin
 Wesley Griffin
 Kevin Keller (University of Maryland)
 Earl Bellinger (SUNY Oswego)
 Alicia Ouyang (River High School)
 Jeffrey Bullard (NIST EL)
 Edward Garboczi (NIST EL)
 Paul E. Stutzman (NIST EL)

<http://www.nist.gov/itl/math/hpcvg/hydrationvis.cfm>

When cement powder is mixed with water, the hydration process that transforms the paste from a fluid suspension into a hardened solid involves complex chemical and microstructural changes. Understanding and predicting the rates of these changes is a longstanding goal, which could lead to the development and deployment of chemical admixtures for controlling early stage properties of concrete.

Computational modeling of this hydration process is challenging because it involves a large number of coupled nonlinear rate equations that must be solved in

a highly irregular three-dimensional domain. To address these challenges we are applying a new computational model called HydratiCA, which has several advantages. HydratiCA uses stochastic cellular automata algorithms to simultaneously model reaction and transport phenomena in 3D. This allows us to track the detailed kinetics and equilibria that occur in a diverse range of cementitious systems.

Parallelization of the model is important so that we can simulate systems that are large enough to be realistic, avoiding finite size effects, and still be able to complete the simulations in a reasonable amount of time. Over the course of the simulation time, a series of data volumes is produced at the time values of interest. Visualization of the output is important both for validation and to understand the results.

This year we submitted a proposal to NSF for computer time and were awarded 100000 hours on the Texas Advanced Computing Center's Dell PowerEdge C8220 Cluster with Intel Xeon Phi coprocessors (Stampede). We set up and validated HydratiCA on Stampede. We made modifications to the code to make it more efficient. We also made progress on checkpointing. We developed an extendable tool for analyzing the output files. It takes a directory of output files and runs a variety of user selected analyses in parallel on the files. One of the analyses generates percolation paths, for which we created an automatic 3D visualization. We have been exploring the use of D3¹⁹ as an additional analysis tool for this project. In particular, we have developed the infrastructure to connect javascript based web apps to the immersive environment to enable interactive analyses using D3.

We also upgraded the physics in the model to include a more general rate law for mineral dissolution in water, with the result applied to simulate the hydration and microstructure development of tricalcium silicate, the most important mineral phase in Portland cement. Dissolution rates obtained from this simulation were in excellent agreement with recent experimental measurements reported in the literature. In addition, the new rate law provides a much better agreement between the simulations and experimental measurements of the time-dependent chemical composition of the aqueous solution during hydration.

With this improved accuracy, we have begun to model the influence on tricalcium silicate hydration of sulfate and carbonate components in solution. This is an important but poorly understood area that has an impact on the well-known effects of gypsum additives and calcite fillers to modify the hardening process. Understanding the mechanisms of optimized gypsum and the filler effect will help enable the rational design of sustainable infrastructure materials with a more be-

¹⁸ <http://www.top500.org>

¹⁹ <http://d3js.org/>

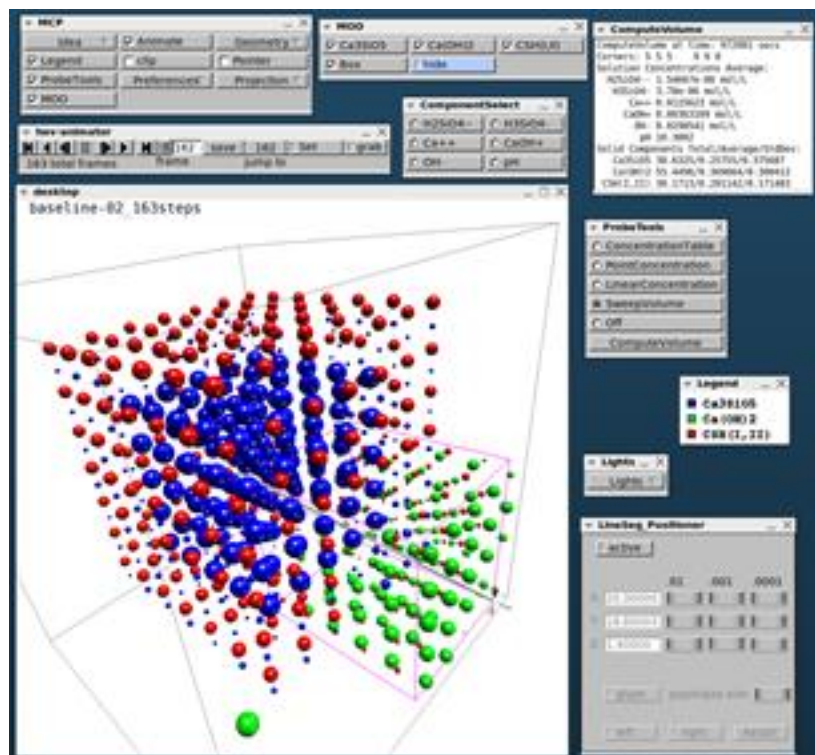


Figure 32. Example of the probe defining a sub-volume and computed total, average, and standard deviation for data items in the selected sub-volume. Tricalcium silicate particles (blue), were hydrated in a lime solution for 20 hours. The particles partially dissolved and are covered with a 0.6-micrometer overgrowth layer of a calcium silicate hydrate product (red). Portlandite (green) nucleates and grows in the adjacent solution.

nign environmental footprint, lower embodied energy, and more efficient integration of industrial byproducts.

A new visualization approach was also implemented this year. Solid components are represented by GPU-rendered sphere glyphs with diameters representing the local volume fraction. The sphere glyphs are displayed at their locations and their diameters are animated over the simulation time. Multiple interactive probes have been implemented to obtain volume data:

- Print a table of all solution and solid component values at that location and time.
- Continuously display the solution components concentration fraction (SCC) value for a selected component while plotting SCC values vs. time.
- Define two end points of an interactive 3D line segment and dynamically plot SCC values along the line segment.
- Use an interactive line segment sweep to identify a sub-volume, and then click a menu item to compute and display total, average and standard deviation for local data items. See Figure 32.

In the coming year we will expand the computations to include larger systems with more realistic particle size and shape distributions. These simulations are important for understanding the possible effects of

space filling by solid hydration products on the kinetics of hydration and rate of hardening of concrete binders.

[1] L. Valentini, J. W. Bullard, G. Artioli, S. G. Satterfield, J. E. Terrill and M. Magistri, Role of Sulfate Incorporation in C-S-H during Cement Hydration: Results from Numerical Modeling of the System C3S + Gypsum, in preparation.

[2] G. W. Scherer, J. W. Bullard and J. J. Thomas, Supersaturation of C-S-H during Hydration of Cement, in preparation.

[3] J. Stoian, T. Oey, J. Huang, A. Kumar, J. W. Bullard, M. Balonis, S. G. Satterfield, J. E. Terrill, N. Neithalath and G. Sant, Prehydration of Ordinary Portland Cement and its Mitigation using Limestone: New Insights from Experiments and Simulations, in preparation.

[4] T. Oey, A. Kumar, J.W. Bullard, N. Neithalath and G. Sant, The Filler Effect: the Influence of Filler Content and Surface Area on Cementitious Reaction Rates, *Journal of the American Ceramic Society* **96** (2013), 1978-1990.

High Precision Calculations of Fundamental Properties of Few-Electron Atomic Systems

James S. Sims

Stanley Hagstrom (Indiana University)

M. B. Ruiz (University of Erlangen)

NIST has long been involved in supplying critically-evaluated data on atomic and molecular properties such as the atomic properties of elements in the Periodic Table and the vibrational and electronic energy level data for neutral and ionic molecules contained in the NIST Chemistry WebBook. Fundamental to this endeavor is the ability to predict, theoretically, a property more accurately than even the most accurate experiments. It is our goal to be able to accomplish this for few-electron atomic systems.

The mathematical intractability of the Schrödinger equation has prevented the computation of accurate numerical solutions for atomic and molecular systems until recently. In the past two decades, there have been breathtaking improvements in computer hardware and

innovations in mathematical formulations and algorithms, leading to “virtual experiments” becoming a more and more cost-effective and reliable way to investigate chemical and physical phenomena.

The essential flaw in theoretical methods is their inability to correctly describe the behavior of many-body wave functions in regions of close electron proximity, the so-called electron cusp region of the exact electronic wave function [1-3]. This flaw leads to incomplete accounting of instantaneous, short-range correlation among electrons. We are undertaking the theoretical development of our hybrid Hylleraas-CI (Hy-CI) wave function method to solve the electron cusp problem and bring sub-chemical accuracy to atomic systems with more than two electrons.

Our method has been employed over the past few years to explore its utility for both three electron lithium systems and the four electron beryllium atom. In the case of lithium, we have computed the lowest four excited state energies of the lithium atom to two orders of magnitude more accurately than has been done before [4]. At the four electron level, we have demonstrated the ability of Hy-CI calculations to achieve 0.1 microhartree accuracy for beryllium. This represents one of the highest levels of accuracy ever achieved in quantum computations with more than three electrons.

Familiar chemical electron affinities and ionization energies involve these nonrelativistic energies. To get truly accurate chemical properties like these it is important to go beyond the 0.1 microhartree accuracy to somewhere close to the nanohartree level we were able to achieve for lithium. To enable Hy-CI calculations to do this, we have been investigating more flexible atomic orbital basis sets, better configuration state function filtering techniques to control expansion lengths, and improved four electron integral techniques. Progress to date has included improving our beryllium accuracy an order of magnitude, and we have computed the non-relativistic energy of not only beryllium, but many members of its isoelectronic series to 8 significant digit accuracy. With these results and a least squares fit of the calculated energies, we have been able to compute the entire beryllium isoelectronic sequence and are in the final stages of preparing a paper on this work.

- [1] T. Kato, On the Eigenfunctions of Many-particle Systems in Quantum Mechanics, *Communications in Pure and Applied Mathematics* **10** (1957), 151-177.
- [2] R. T. Pack and W. B. Brown, Cusp Conditions for Molecular Wavefunctions, *Journal of Chemical Physics* **45** (1966), 556-559.
- [3] W. Kutzelnigg and J. D. Morgan III, Rates of Convergence of the Partial-wave Expansions of Atomic Correlation Energies, *Journal of Chemical Physics* **96** (1992), 4484-4508.
- [4] J. S. Sims and S. A. Hagstrom, Hy-CI Study of the 2

Doublet S Ground State of Neutral Lithium and the First Five Excited Doublet S States, *Physical Review A* **80** (2009), 052507.

- [5] J. S. Sims and S. A. Hagstrom, Hylleraas-Configuration Interaction Study of the Singlet S Ground State of Beryllium., *Physical Review A* **83** (2011), 032518.
- [6] James S. Sims and Stanley A. Hagstrom, Hylleraas-configuration-interaction Nonrelativistic Energies for the Singlet S Ground States of the Beryllium Isoelectronic Series up through $Z = 113$, in preparation.

Nano-structures, Nano-optics, and Controlling Exciton Fine Structure

James S. Sims

Wesley Griffin

Garnett W. Bryant (NIST PL)

Jian Chen (University of Maryland Baltimore County)

Research and development of nanotechnology, with applications ranging from smart materials to quantum computation to biolabs on a chip, is an important national priority. Semiconductor nanoparticles, also known as nanocrystals and quantum dots, are one of the most intensely studied nanoscale systems. Nanoparticles are typically 1 nm to 10 nm in size, with a thousand to a million atoms. Precise control of particle size, shape and composition allows one to tailor charge distributions and control quantum effects to tailor properties completely different from the bulk and from small clusters. As a result of enhanced quantum confinement effects, nanoparticles act as artificial, manmade atoms with discrete electronic spectra that can be exploited as light sources for novel enhanced lasers, discrete components in nanoelectronics, qubits for quantum computers, and enhanced ultrastable fluorescent labels for biosensors to detect, e.g., cancers, malaria or other pathogens, and to do cell biology.

We are working with the NIST Physical Measurement Laboratory to develop computationally efficient large scale simulations of such nanostructures, as well as to develop immersive visualization techniques and tools to enable analysis of highly complex computational results of this type. The electrical and optical properties of semiconductor nanocrystals and quantum dots are studied. In the most complex structures, this entails modeling structures with on the order of a million atoms. Highly parallel computational and visualization platforms are critical for obtaining the computational speeds necessary for systematic, comprehensive studies.

This year our work, which was focused on modulating and controlling the optical properties of self-assembled quantum dots using electric fields [1], culminated in a paper published in *Physical Review B* [2].

Calculations were carried out on NIST's 7,892-processor Linux cluster. In addition to the electric field work, we have also added a parameter to the code which handles the imaginary part of the magnetic field parameters (electric field parameters are real), and there are now data input files for strain, electric fields, and magnetic fields. Magnetic fields are an invaluable tool that allows for the implementation of two-level systems in quantum dots, with the control of spin needed for applications in quantum information. A fully atomistic theory has been shown to be essential for a full description of exciton states in quantum dots in strain and electric fields. We have implemented an atomistic, tight-binding theory for excitons in quantum dots with an applied magnetic field. A talk was given on this work at the 13th Annual International Conference of Optics of Excitons in Confined Systems [3].

As the computational model has been extended to handle more complex and larger systems by including not only the nanostructures but also the substrate and environment around them, parallel processing has become even more of a necessity. Both shared memory OpenMP parallelization and distributed memory MPI are employed. In the coming year we will continue to focus on modulating and controlling the optical properties of self-assembled quantum dots via external magnetic fields using this new feature of our codes.

We have been working on visualizing new data sets as part of a recent NIST cooperative agreement with the University of Maryland Baltimore County in which Dr. Jian Chen and her students will explore new methods for data visualization in 3D immersive virtual environments. The results of this work should provide insight into quantum dots and electron spin distribution. Additionally, since this new data is a 3D vector field, the tools we develop should be useful for vector field data in the future.

Going forward, our plan is to develop Dr. Chen's preliminary visualizations into a 3D immersive visualization application that can be used on a workstation and in the RAVE. We also plan to submit a paper on this work to the 2014 IEEE VIS Conference.

- [1] G. W. Bryant, N. Malkova and J. S. Sims, "Electric-field Control of Exciton Fine Structure: Atomic Scale Manipulation of Exchange Splitting," American Physical Society Annual March Meeting, Baltimore, MD, March, 2013.
- [2] G. W. Bryant, N. Malkova and J. S. Sims, Mechanism for Controlling the Exciton Fine Structure in Quantum Dots using Electric Fields: Manipulation of Exciton Orientation and Exchange Splitting at the Atomic Scale, *Physical Review B* **88** (2013), 161301(R).
- [3] G. W. Bryant and J. S. Sims, "Magnetoexcitons in Quantum Dots: Atomistic Theory of g-factors, Diamagnetic Shifts and Spin Mixing", 13th International Conference on Optics of Excitons in Confined Systems, Rome, Italy, Sept 9-13, 2013.

Parallel Adaptive Refinement and Multigrid Finite Element Methods

William F. Mitchell

Marjorie A. McClain

Eite Tiesinga (NIST PML)

Paul Julienne (NIST PML)

John Villarrubia (NIST PML)

<http://math.nist.gov/phaml>

Finite element methods using adaptive refinement and multigrid techniques have been shown to be very efficient for solving partial differential equations (PDEs). Adaptive refinement reduces the number of grid points by concentrating the grid in the areas where the action is, and multigrid methods solve the resulting linear systems in an optimal number of operations. Recent research has been with *hp*-adaptive methods where adaptivity is in both the grid size and the polynomial order of approximation, resulting in exponential rates of convergence. W. Mitchell has been developing a code, PHAML, to apply these on parallel computers. The expertise and software developed in this project are useful for many NIST laboratory programs, including material design, semiconductor device simulation, the quantum physics of matter, and simulation of scanning electron microscopes.

Recently we completed a study of the performance of 13 proposed *hp*-adaptive strategies in terms of accuracy vs. degrees of freedom [3]. This year we extended the experiment to include a comparison based on accuracy vs. computation time [1]. For this experiment we gathered a collection of 12 test problems, most of which came from the numerical results section of papers on *hp*-adaptive refinement. These problems contain a variety of difficulties including singularities, sharp peaks, wave fronts, oscillations and boundary layers. Most of them are parameterized to adjust the strength of the difficulty. We found that which strategy is most effective depends on the type of difficulty, and the accuracy requirements. The so-called reference solution methods performed well in terms of accuracy vs. degrees of freedom, but are very expensive computationally. In terms of accuracy vs. computation time, the use of *a priori* knowledge is best for problems with known singularities and no other significant feature, while the method based on the decay rate of the coefficients of the *p*-hierarchical basis seems to be the best general purpose strategy.

The 12 test problems used in the study are all two-dimensional linear elliptic PDEs. We believe it would be useful to create a collection of standard benchmark PDEs, appropriate for adaptive mesh refinement, of other types, including 3D, parabolic, hyperbolic, and nonlinear equations. We have begun work on a web

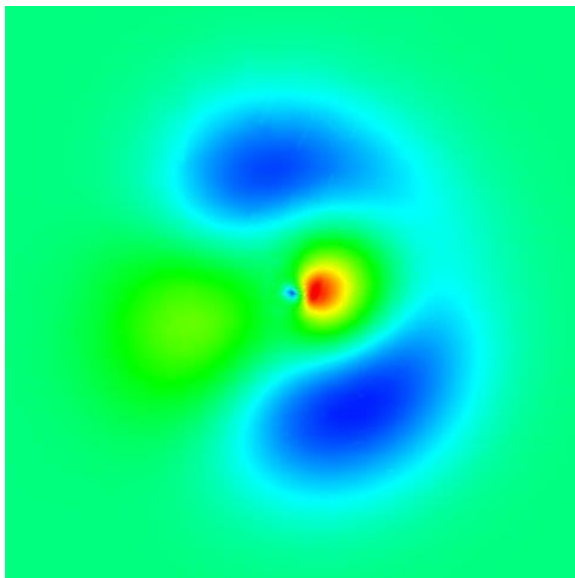


Figure 33. Slice along the $z=0$ plane of the fourth wave function from a 3D simulation of the interaction of two nonreactive polar RbCs molecules.

site²⁰ to make such a collection available to the adaptive finite element research community [2].

The development and application of PHAML continues to be of prime importance. PHAML was originally developed to solve elliptic partial differential equations in two spatial dimensions. We are now extending it to three dimensions, in support of collaborations with PML. This year we extended the code to include high order tetrahedral elements, but have not yet included *hp*-adaptivity with those elements.

There are two major collaborative efforts with PML that apply PHAML to their physical models.

- In collaboration with Eite Tiesinga and Paul Julienne, we are using PHAML to study the interaction of atoms and molecules held in an optical trap. Previously we calculated the bound states, scattering properties and dynamics of two dipolar molecules held in a cylindrically symmetric trap, a 2D problem [4]. We are currently extending these simulations to a 3D model without the assumption of cylindrical symmetry. We validated PHAML's high order 3D elements using the harmonic oscillator problem, for which the exact wave function is known. Using 4th order elements we were able to get six-digit accuracy in a few minutes. We are now attempting to solve a much more difficult problem, a model of two nonreactive polar RbCs molecules in an optical lattice site.

- We are collaborating with John Villarrubia to apply PHAML to the modeling of scanning electron microscope images of samples that contain a mixture of conducting and insulating regions. Villarrubia has a code that models electron scattering in materials, secondary electron production, and detection. We have coupled this code with PHAML to determine the electric fields that affect the image.

Future work will continue to enhance PHAML with additional capabilities, robustness and efficiency, implement and study some recently proposed *hp*-adaptive strategies, develop a new *hp*-adaptive strategy that attempts to capture the essential aspects of the reference solution strategies without computing the expensive reference solution, complete the extension of PHAML to 3D problems, and continue collaborations that use PHAML in NIST applications.

- [1] W.F. Mitchell and M.A. McClain, A Comparison of *hp*-Adaptive Strategies for Elliptic Partial Differential Equations, *ACM Transactions on Mathematical Software*, to appear.
- [2] W.F. Mitchell, A Collection of 2D Elliptic Problems for Testing Adaptive Algorithms, *Applied Mathematics and Computation* **220** (2013), 350-364.
- [3] W.F. Mitchell, Performance of *hp*-Adaptive Strategies for Elliptic Partial Differential Equations, in *Proceedings of the 4th International Congress on Computational Engineering and Sciences (FEMTEC 2013)*, May 2013.
- [4] T.M. Hanna, E. Tiesinga, W.F. Mitchell and P.S. Julienne, Resonant Control of Polar Molecules in an Optical Lattice, *Physical Review A* **85:2** (2012).

Texture Compression Evaluation and Optimization

Wesley Griffin

Marc Olano (Univ. of Maryland Baltimore County)

Texture compression is widely used in real-time rendering to reduce storage and bandwidth requirements. Hardware-based texture compression has not fundamentally changed since its introduction in 1999. Recently, however, interest has grown in improving texture compression. We are exploring new techniques for reducing the bit rate for the current fixed bit rate algorithms as well as new variable bit rate algorithms that can be efficiently decoded in graphics hardware.

In evaluating texture compression, the most common approach is to use some combination of the mean square error, peak signal-to-noise ratio, or visual image inspection of the compressed texture. In [1] we show that this approach for evaluating texture compression does not properly account for the two ways in which

²⁰ <http://math.nist.gov/amr-benchmark>

textures are used in rendering images, and present a method that evaluates compression artifacts on final rendered images using perceptually rigorous objective image quality assessment metrics.

One of the more interesting conclusions in our paper is that current hardware compression algorithms are too conservative. Further reductions in bit rate can reduce the compressed size of textures while having only a small impact on image quality. This result benefits the real-time rendering community by showing that individual textures can be more highly compressed, thus saving on bandwidth and asset load times.

Going forward, we plan to turn our evaluation framework into an optimization function for texture compression. By developing an optimization method we can enable real-time rendering asset pipelines to automatically optimize texture compression rates and quality. This will further benefit the real-time rendering community by removing the highly subjective and time-consuming task of finding the right compression algorithm settings for textures.

- [1] W. Griffin and M. Olano, Objective Image Quality Assessment of Texture Compression, in *Proceedings of the 2014 ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games*, to appear.

Declarative 3D Graphics

Sandy Ressler

Kyle Leber (Lock Haven University)

Web pages exist as large collections of hierarchical elements that are rendered to the page. All content is organized via the Document Object Model (DOM). A huge collection of tools has been created to allow programmers to manipulate the DOM. In particular, tools and frameworks based on JavaScript have become the go-to language for Web development. Declarative 3D Graphics is a method of representing graphics in a declarative manner (as opposed to imperative) that makes 3D graphics a first class citizen of the web page. Placing 3D graphics in the DOM, therefore, allows these same JavaScript tools to access and manipulate 3D graphics, even though they were not specifically designed for 3D graphics.

We use anthropometry, the measurement of humans, as a testbed application, to experiment with declarative 3D capabilities and techniques. This application enables us to visualize several hundred whole body laser scans complete with the 3D landmarks that were captured as part of an anthropometric survey. Over the last 18 months we have extended this application to let us take direct measurements, interactively, on the surface of the visualized bodies. We plan on extending the capabilities of JavaScript libraries, such

as jQuery, to provide a useful set of capabilities for the use of anthropometric databases.

Of note is the fact that we do not need to develop yet another entirely new set of user interface techniques; we can simply use the commonly understood vocabulary of web pages. The illustration demonstrates use of our application in a typical web browser. This demonstrates that current declarative 3D technology is viable for the development of larger scale applications using the infrastructure that already exists for web application development. We hope to extend the visual measurement capabilities to more dimensions such as the ability to take and measure cross sections through the body and volumetric measurements.

- [1] J. Jankowski, S. Ressler, J. Behr, Y. Jung, K. Sons and P. Slusallek, Declarative Integration of Interactive 3D Graphics into the World-Wide Web: Principles, Current Approaches, a Research Agenda in *Web3D '13: Proceedings of the 18th International Conference on 3D Web Technology*, San Sebastian, Spain, June 20-22, 2013, 39-45.
- [2] S. Ressler and K. Leber, Web Based 3D Visualization and Interaction for Whole Body Laser Scans, in *Proceedings of the 4th International Conference and Exhibition on 3D Body Scanning Technologies*, Long Beach CA, Nov. 19-20, 2013.



Figure 34. Testbed application for declarative 3D graphics on the web.

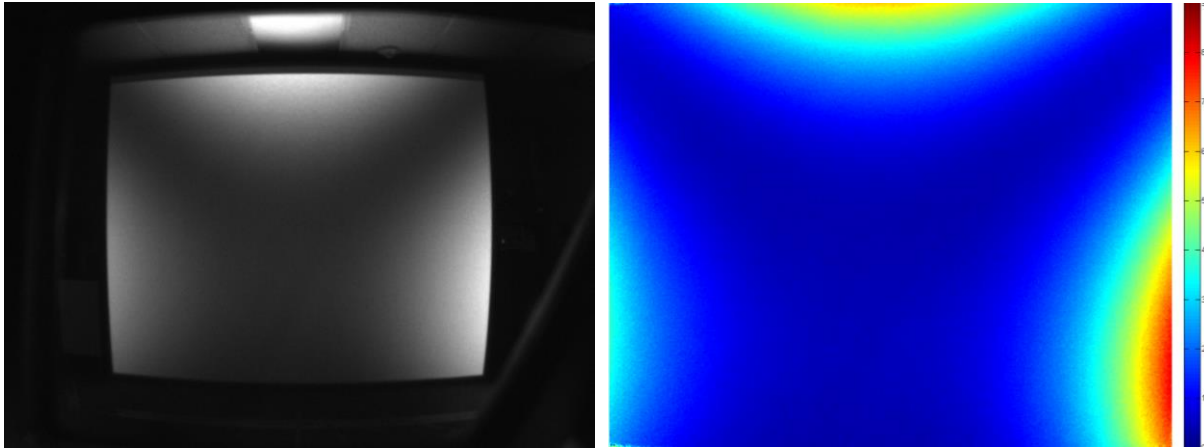


Figure 35. Left image shows view of 3D display observed through left lens of eye glasses. The right image is a map of the 3D crosstalk over the active area of the display.

Optical Characterization of Immersive 3D Displays

S. Satterfield

J. E. Terrill

J. Penczek (NIST PML)

P. A. Boynton (NIST PML)

T. Scheitlin (NCAR)

Many things influence a visualization of a dataset. These include the nature of the data itself and its uncertainties, the visual representation space, the visualization algorithms used for implementation, as well as algorithmic simplifications. Another factor impacting the final visualization is how accurately the images are rendered by the display system. We seek to develop a deeper understanding of each part of this process. In the current work we are studying the impact of the display on stereo visualizations.

Every display technology has its own inherent performance limitations. The non-ideality of the display introduces constraints on what information can actually be observed by the viewer. By characterizing the optical performance of the display system, we can quantitatively determine what visual information may be impaired. The operators of the display facility can use the results to evaluate how the visual characteristics that are important to them are affected, understand the visual limitations of their system, and use the performance data to drive improvements. The display performance data also informs the scientists that create the visualization data how much of that data can actually be realized/observed. For example, the display may exhibit sufficient 3D crosstalk that small spatial features are washed out due to a lack of contrast. If the scientists are aware of this limitation, they can modify their visualization to work around that limitation. A careful characterization of the display system can also

predict if the display is prone to inducing visual fatigue or headaches.

This past year we leveraged our prior work to develop a suite of tests for the optical characterization of immersive 3D displays [1-3]. A set of 23 image pairs and a custom detector gimbal alignment structure were created to support this study. A precision spectroradiometer (Photo Research PR-740) with a 1-degree aperture, and a 4 nm bandwidth, was used to measure radiometric, photometric, and colorimetric data on two immersive stereo display systems. One was a rear-projection system, the other a front-projection system. The optical characteristics measured on these systems included: luminance and color difference between left and right eye, contrast ratio between left and right eye, crosstalk between left and right eye, viewing direction dependence, head tilt dependence, luminance and color uniformity, and shutter glasses characteristics. A relative photometric camera was also used to evaluate the spatial distribution of some of these characteristics. The 2D maps captured by the camera can provide an intuitive and comprehensive description of how these characteristics behave across the viewing area [4].

An example of this is given in Figure 35 for the case of 3D crosstalk from the display system at the NIST Boulder Visualization Lab. The image on the left illustrates what the viewer can observe for an intended black image at the left eye, with a white unintended image in the right eye. In an ideal 3D display, only a pure black image should be observed in the left eye. However, real displays will exhibit some light leakage from the white unintended image to the black intended image. The images in Figure 35 demonstrate how the light leakage is distributed over the screen, and serves to degrade the performance of the display. The 2D map on the right quantifies the 3D crosstalk over the entire display. Further measurements revealed that the “X” crosstalk pattern rotates with a corresponding head tilt, suggesting, therefore, that much of this crosstalk is

related to the imperfections of the eye glasses.

The first display tested was the NIST Powerwall display in Boulder, Colorado. This was a rear projection display with a Christie Mirage 2000 projector, an 8.75 m × 6.79 m active screen, with 1280×1024 resolution, and Crystal Eyes3 active glasses. In most cases, the viewers of this display stand about 1.2 m in front of the screen and wear the active 3D glasses. The same viewing conditions were replicated for the measurements by placing the detector at the same eye location. Our investigation revealed that the Boulder system had a relatively low luminance, which limited the contrast of the data and required a dark room for viewing. The eye glasses were the dominant cause of the 3D crosstalk, had poor optical transmission, and blue-shifted the colors. The display system also exhibited a perceptible flicker, which increased the propensity for eye fatigue and headaches with prolonged viewing.

The second display system investigated was at the National Center for Atmospheric Research (NCAR) Visualization Lab. The laboratory uses the display system to present 3D datasets on climate research, and as an educational outreach tool. This front projection system had a Christie Mirage HD6 projector with 1920×1080 resolution, a 3.78 m × 2.13 m active screen area, and used Macnaughton active 3D glasses. The screen was mounted on a wall at the front of a conference room, with the viewers seated around a U-shaped table centered in front of the screen. Given the wide range of viewing angles, the detector was nominally positioned normal to the screen and 5.4 m from the screen center, which approximated the average viewing conditions. The display exhibited brighter images than the NIST Boulder system, which contributed to substantial improvements in the visibility of features. The eye glasses were still the dominant cause for the 3D crosstalk, but to a much lesser degree. The glasses also had better optical transmission, yet still produced a color shift. In addition, the open front-projection configuration of the NCAR system allowed us to characterize the relative contribution of the projector, screen, and eye glasses to the final viewing experience. Some limiting characteristics were identified and quantified. The room lighting conditions were also evaluated and shown to have a dramatic impact on how much visual information could be observed.

The preliminary findings of this investigation were provided to both Visualization Lab supervisors. It is expected that this information will be used to direct future improvements to these facilities. In the coming year, a more detailed analysis of this investigation will be submitted to a relevant journal in order to raise awareness of the practical limitations of rendering complex visual information. We also intend to extend this work to multi-screen immersive displays, such as a four-sided Cave Automatic Virtual Environment (CAVE) display system. This is a more immersive vir-

tual reality environment, which also poses a more complex rendering and measurement challenge.

- [1] Information Display Measurements Standard²¹, International Display Metrology Committee, Society of Information Display.
- [2] E. F. Kelley, K. Lang, L. D. Silverstein and M. H. Brill, Methodology for Estimating the Luminous Flux Based upon Color Primaries from Digital projection Displays, NISTIR 6657, January 2009.
- [3] E. F. Kelley, K. Lang, L. D. Silverstein and M. H. Brill, Projector Flux from Primaries, *Society of Information Display Symposium Digest of Technical Papers* **40** (2009), 224-227.
- [4] J. Penczek, P. A. Boynton, E. F. Kelley, Measuring 3D Crosstalk Uniformity and its Influence on Contrast Ratio, *Journal of the Society of Information Display* **21** (June 2013), 225-230.

Visualization for Measurement Science for Complex Information Systems

Sandy Ressler

Kevin Mills (NIST ITL)

Chris Dabrowski (NIST ITL)

James Filliben (NIST ITL)

We aim to develop and evaluate a coherent set of methods to understand behavior in complex information systems, such as the Internet, computational grids and computing clouds. ACMD is providing visualizations of simulation results that are being undertaken as part of this effort. One key goal is to produce these visualizations as rapidly as possible in order to provide insight to the researchers early enough in development to positively affect the research. On several occasions we have, in fact, been instrumental in identifying bugs in the simulation system.

For example, we produced an animation illustrating the progression of “fitness” of a model evolved using a genetic algorithm applied to the Koala cloud computing simulation system. The animation uses shape, size and color as a method to illustrate the settings of three variables in the simulation. Each generation, from the 500 total, corresponds to a single frame of the animation. See Figure 36.

In addition, the researchers are beginning to study a network based on the 2001 configuration of the Autonomous System portion of the Internet (see Figure 37). The graph consists of approximately 11000 nodes and 47000 edges. Using an off-the-shelf open source tool (gephi) we produced visualizations that helped

²¹ <http://icdm-sid.org/>

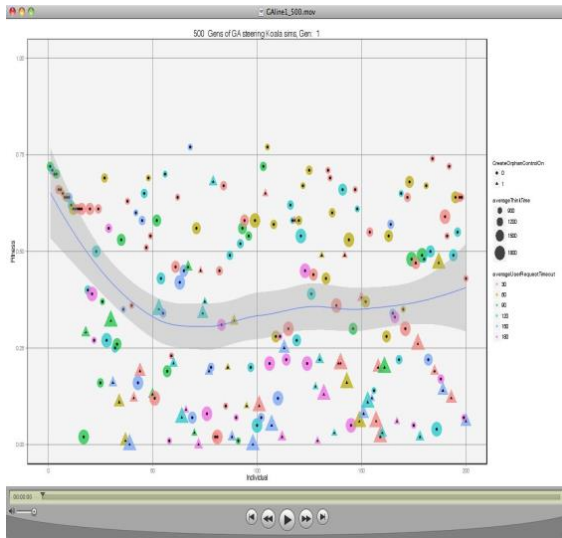


Figure 36. Frame from an animation illustrating the effect of settings from 3 variables on the fitness of the individuals. The gray snake like line illustrates the quickly increasing fitness.

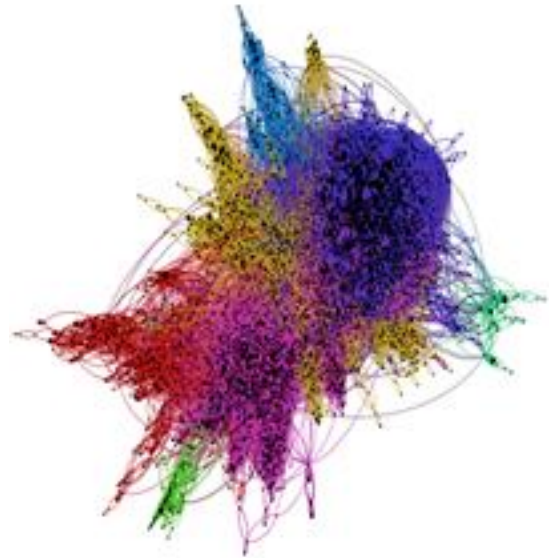


Figure 37. Internet autonomous system graph circa 2001.

identify structure in the network which was completely unknown previously. Each color is a particular cluster of nodes is computed according to the “modularity” network metric.

- [1] K. Mills, C. Dabrowski, J. Filliben and S. Ressler, Using Genetic Algorithms and Simulation to Search for Failure

Scenarios in System Models, in *Proceedings of the Fifth International Conference on Advances in System Simulation (SIMUL 2013)*, October 27 - November 1, 2013, Venice, Italy.

Mathematical Knowledge Management

We work with researchers in academia and industry to develop technologies, tools, and standards for representation, exchange, and use of mathematical data. Of particular concern are semantic-based representations which can provide the basis for interoperability of mathematical information processing systems. We apply this to the development and dissemination of reference data for applied mathematics. The centerpiece of this effort is the Digital Library of Mathematical Functions, a freely available interactive and richly linked online resource, providing essential information on the properties of the special functions of applied mathematics, the foundation of mathematical modeling in all of science and engineering.

Digital Library of Mathematical Functions

Daniel Lozier

Frank Olver

Bruce Miller

Bonita Saunders

Marjorie McClain

Howard Cohl

Ronald Boisvert

Charles Clark (NIST PML)

Brian Antonishek (NIST ITL)

Adri Olde Daalhuis (University of Edinburgh)

<http://dlmf.nist.gov/>

Math and science go hand in hand. Purely mathematical developments find application in practical problem-solving in all fields of science as well as engineering, while cutting-edge science is a major driver of mathematical research. Often the mathematical objects at the intersection of math and science are *mathematical functions*. Effective use of these tools requires ready access to their many intricate properties. This need was capably satisfied for 50 years by the *Handbook of Mathematical Functions* [1]. Twenty-first century needs, greatly enlarged since 1964, are being met by the *NIST Digital Library of Mathematical Functions*²² (DLMF) and its print companion, the *NIST Handbook of Mathematical Functions* [2]. The new handbook contains more than twice as many formulas as the old one, coverage of more functions, and an up-to-date list of references. Collectively, the new handbook and website are called the DLMF. The website covers everything in the handbook and much more: additional formulas and graphics, interactive search, live zooming and rotation of 3D graphs, internal links to symbol definitions and cross-references, and external links to online references and sources of software.

Today's DLMF is the product of many years of effort by more than 50 expert contributors. But its appearance in 2010 was not the end of the project. Corrections to confirmed errata, bibliographic updates, and

addition of important new material all need to be made, and new chapters covering emerging subject areas need to be added, so as to assure the continued vitality of the DLMF deep into the 21st century. Related developments currently in progress at NIST include DLMF Tables, an on-demand table generation web service for special functions, and the DRMF (Digital Repository of Mathematical Formulae), a listing of mathematical formulas taken with permission from respected publications such as Gradshteyn and Ryzhik's *Tables of Integrals, Series and Products*.

Just one update appeared on the website in the past year. It introduced several improvements that affect display of math and graphics. A short list of corrections and other changes are scheduled for the next release, expected in early 2014. The complete record of changes since original release is given online²³.

The DLMF project has been led by senior editors with the expert assistance of associate editors, chapter authors, and chapter validators. With the passage of time some of these experts, for various reasons, have reduced or ended their commitment to the project. A major blow to the project was the death of the Mathematics Editor, Frank Olver, in April 2013; fortunately, Adri Olde Daalhuis had already been named as a second Mathematics Editor. Another recent death was Bille Carlson, long-time professor at Iowa State University and author of the chapter on Elliptic Integrals.

As a result of these developments, leadership of the DLMF project is being reconstituted into three newly defined categories: the *editorial board*, a small group of senior leaders with ultimate responsibility and final authority for the content and presentation of the DLMF, *senior associate editors*, senior leaders in the community with special interest in special functions, mathematical handbooks, and the presentation of mathematics on the web who will advise the editorial board on the future development of the DLMF, and *associate editors*, experts in the mathematics of special functions who will assist the Mathematics Editor with the maintenance and development of the technical content of the DLMF. All former associate editors, authors, and validators have received a letter signed by ITL Director

²² <http://dlmf.nist.gov/>

²³ <http://dlmf.nist.gov/errata>

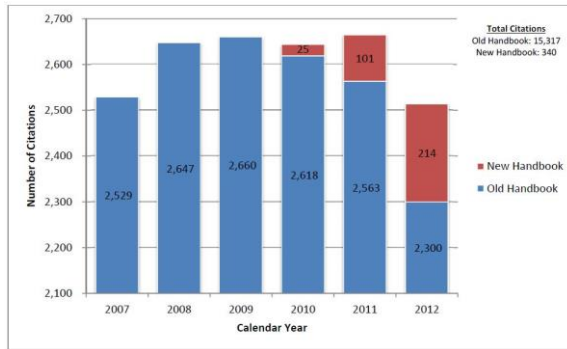


Figure 38. Citations to the original Abramowitz and Stegun Handbook and the DLMF compared.

Charles Romine describing the new editorial structure. The recipients were asked if they wish to offer to continue their participation in one of these new categories. They were asked also if they know of mathematicians whom they would recommend to serve in one of the categories. An upcoming editorial meeting will be devoted to reviewing responses to the letter and filling in the new categories of leadership.

The NIST Information Services Office has conducted a citation analysis to measure the penetration of the DLMF into the user community in comparison to the old 1964 Abramowitz-Stegun handbook, which the DLMF is intended to replace. The analysis covers the years 2007-2012, roughly 3 years before and 3 years after publication of the DLMF. The data shown in Figure 38 combines the handbook and website citations for the DLMF (It was reported in the study that 17% of the citations over the 3-year period were to the online version.) It can be seen from the figure that citations to the DLMF began immediately to increase steadily from year to year, while citations to the old handbook, which had been increasing, began a steady decrease in 2010. In percentage terms, by the end of 2012 citations to the DLMF handbook and website had grown to about 8% of the total number of citations to both handbooks.

- [1] M. Abramowitz and I. Stegun, eds., *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*, Applied Mathematics Series **55**, National Bureau of Standards, Washington, DC, 1964.
- [2] F. Olver, D. Lozier, R. Boisvert and C. Clark, eds., *NIST Handbook of Mathematical Functions*, Cambridge University Press, 2010.

Mathematical Knowledge Representation

Bruce Miller

Deyan Ginev (Jacobs University, Germany)

Although we became involved in Mathematical Knowledge Management (MKM) to support the development of the Digital Library of Mathematical Functions (DLMF), the release of the latter in 2010 hardly signified an end to our activities. Simply maintaining the DLMF [1] requires continued enhancement of the tools and techniques as well as tracking the technologies involved. Applying what we've learned to other projects is an even more powerful motivator.

Mathematics Markup Language (MathML) is at the core of delivering mathematics on the web, and the current mixed situation illustrates some of our challenges. MathML defines markup for both *Presentation* (for displaying mathematics) and *Content* (for encoding its meaning). We participate in the Math Working Group of the World Wide Web Consortium (W3C), which recently released version 3 of the MathML specification. This version greatly improves the expressiveness of the Content format. Yet, it is quite difficult to convert markup meant for human consumption, such as LaTeX intended for high-quality typesetting, into fully disambiguated Content MathML.

While Content MathML is essential for reusing mathematics for computation, the more easily generated Presentation MathML at least provides quality display, is scalable, accessible and can be supported by assistive technologies. Consequently, several recent standards, in particular version 5 of HTML (HTML5), the markup used for web pages, and ePub, a standard for electronic books, have both adopted MathML as an integral part of their markup. Furthermore, at World Wide Web Consortium's encouragement, the Math Working group is preparing a 2nd Edition of the MathML 3 specification and will submit it this spring to ISO to become an international standard.

In spite of this, some major browser developers are still reluctant to expend the effort implement MathML; only one browser has essentially full, native support. However, a portable JavaScript library called MathJax can display MathML on most browsers with high quality, albeit quite slowly, while preserving accessibility.

Thus MathML support, one way or another, is much more widespread than it was when DLMF was initially released. The spring 2014 update of DLMF will employ HTML5 as the default format rather than using images for math. This will include MathML; MathJax will be used as the fallback for browsers without native support. Although it may be slower than images in some cases, it will look better, be more scal-

able and accessible and will increase the visibility of MathML (hopefully in a positive way).

In this context, much of this year's work has been in development [2], rather than research. The LaTeXML software, used to convert LaTeX to XML (HTML, HTML5, MathML, etc.) moves towards a



long overdue release. Portability, code quality, robustness and coverage have

been major concerns, as well as encompassing a larger set of standards. Generation of HTML5 has already been mentioned. Prototype support for ePub has also been completed. Some of the graphics libraries commonly used in LaTeX (tikz, pgf) can now be used to produce Scalable Vector Graphics (SVG), a standard for 2D graphics also included in HTML5.

Ongoing progress in generating Content MathML, particularly for DLMF, has enabled extensibility, allowing us to employ more sophisticated parsers. Some groundwork in representing inherently ambiguous markup has also been achieved [3].

In the meantime, the software is being used in the infrastructure of several other projects such as: Planet Math²⁴; it continues to be used to process arXiv²⁵ [4], in particular to generate test-data for research in mathematical search; and in the Digital Repository of Mathematical Formulas (see page 71).

- [1] B. R. Miller, Three Years of DLMF: Web, Math and Search, *Lecture Notes in Computer Science* **7961**, Springer, Heidelberg (2013), 288-295.
- [2] B. R. Miller, D. I. Ginev, LaTeXML 2012 - A Year of LaTeXML, *Lecture Notes in Computer Science* **7961**, Springer, Heidelberg (2013), 335-338.
- [3] D. Ginev, *The Structure of Mathematical Expressions*, Master's Thesis, Jacobs University, 2011.
- [4] H. Stammerjohanns, M. Kohlhase, D. Ginev, C. David, B. Miller, Transforming Large Collections of Scientific Publications to XML, *Mathematics in Computer Science* **3:3** (2010), 299-307.

²⁴ <http://planetmath.org>

²⁵ <http://arxiv.org>

Visualization of Complex Functions Data

Bonita Saunders
 Brian Antonishek (NIST ITL)
 Qiming Wang
 Bruce Miller
 Sandy Ressler
 Daniel Lozier

While complex function data visualization can be a powerful tool for researchers studying mathematical or physical phenomena, problems with accessibility can severely limit its usefulness. Currently, interactive 3D visualizations in the NIST Digital Library of Mathematical Functions (DLMF) are rendered using two common technologies, VRML and X3D, which require users to download a plugin based on their operating system. This is inconvenient not only for users, but also for those maintaining the site, since updates of the plugin, web browser, and even the operating system can affect the quality of the visualization. To remedy this problem we have been working on the conversion of the DLMF 3D graphics to a WebGL format.

WebGL is a JavaScript API (application programming interface) for rendering 3D graphics in a web browser without the use of a plugin. Our WebGL code is based on the X3DOM framework which allows the building of the WebGL application around X3D, an XML based graphics code. WebGL visualizations are visible on Windows, Mac, and Linux platforms in most HTML5 compatible browsers. Microsoft had originally indicated that they would not support WebGL because of security concerns, but they have now relented and are touting it as a feature of their latest browser, Internet Explorer 11 under Windows 8.1. Our preliminary tests and research indicate that there may be some problems with their implementation, but we will continue to monitor this. On the other hand, while we never found a VRML/X3D plugin that would successfully render our complex visualizations in Linux, we have had no problem rendering our WebGL versions of the visualizations in Linux using common web browsers such as Firefox and Chrome.

We have spent the last few months integrating the new visualizations into the DLMF. Figure 39 shows a WebGL visualization of the Riemann zeta function embedded in a DLMF web page. The WebGL renderings of the DLMF visualizations are superior in overall quality to the VRML/X3D versions. Color maps are more vibrant, cutting plane curves clearer, and the interactive movement of surfaces faster and smoother. However, we noticed that WebGL is more particular about the quality of the underlying computational grid. A few color map anomalies not seen in the VRML/X3D visualizations were traced to slight overlaps of grid lines. Subsequently we regenerated several

grids and boundary contours, greatly improving surface color maps and clipping in some WebGL visualizations. We hope the adaptive grid generation work now in progress will help us eliminate minor imperfections still apparent on some surfaces, especially those containing several poles. The WebGL visualizations will appear in the next update of the DLMF web site as the default, but for this first release, users will still be able to choose VRML/X3D visualizations if preferred.

- [1] B. Saunders, Q. Wang and B. Antonishek, Adaptive Composite B-Spline Grid Generation for Interactive 3D Visualizations, in *Proceedings of MASCOT/ISGG 2012*, Las Palmas de Gran Canaria, Spain, October 22-26, 2012, submitted.
- [2] B. Saunders and Q. Wang, Tensor Product B-Spline Mesh Generation for Accurate Surface Visualizations in the NIST Digital Library of Mathematical Functions, *Mathematical Methods for Curves and Surfaces, Lecture Notes in Comp. Science* **5862** (2010), Springer, 385-393.
- [3] B. Saunders and Q. Wang, Tensor Product Grid Generation for Complex Surface Visualizations in a Digital Library of Mathematical Functions, in *Proceedings of the 11th International Society for Grid Generation (ISGG) Conference*, Montreal Canada, May 25-28, 2009, SV.3.
- [4] Q. Wang, B. Saunders and S. Ressler, Dissemination of 3D Visualizations of Complex Function Data for the NIST Digital Library of Mathematical Functions, *CODATA Data Science Journal, Volume 6, 2007 (Supplement on the Proceedings of the 20th International CODATA Conference, Beijing, China, October 2006)*, pp. S146- S154.
- [5] B. Saunders and Q. Wang, From B-Spline Mesh Generation to Effective Visualizations for the NIST Digital Library of Mathematical Functions, in *Curve and Surface Design: Avignon 2006, Sixth International Conference on Curves and Surfaces*, Avignon, France, Nashboro Press, 2007, 235-243.

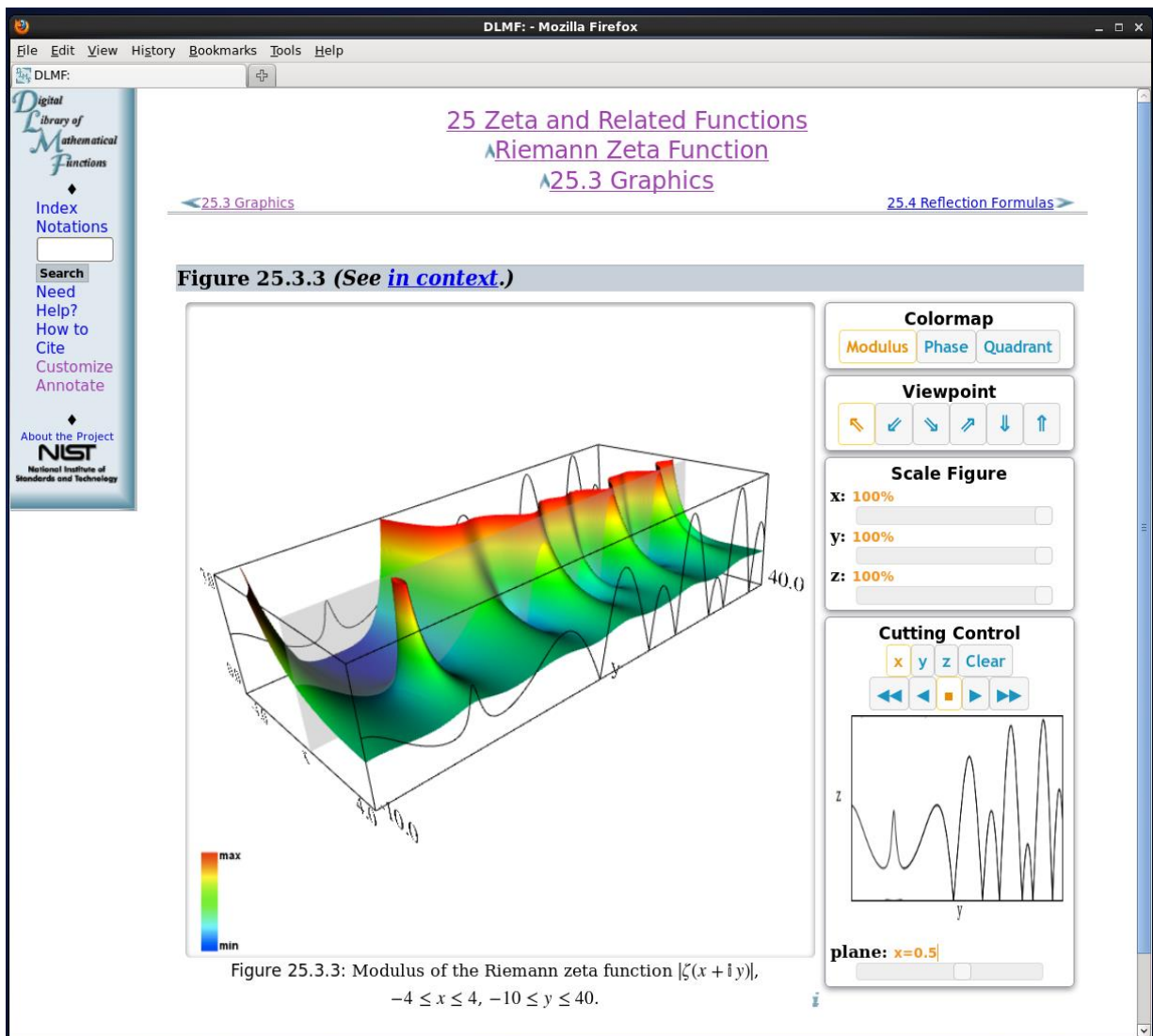


Figure 39. DLMF webpage with embedded visualization of Riemann zeta function.

Standard Reference Tables on Demand

Bonita Saunders

Bruce Miller

Marjorie McClain

Daniel Lozier

Chris Schanzle

Annie Cuyt (University of Antwerp)

Stefan Becuwe (University of Antwerp)

Franky Backeljauw (University of Antwerp)

Tables of elementary and special functions values have been used by mathematical software designers, numerical analysts and other researchers in the mathematical and physical sciences for many years. Reliable reference values are invaluable, for example, when testing new software implementations. Today several libraries and systems produce high quality function values, but most offer limited information about the accuracy of their computations. One notable exception is the work of Annie Cuyt and colleagues at the University of Antwerp [1, 2, 3], whose multiprecision software provides strict error bounds for the accuracy of its computations.

Software designed by the Antwerp group was used to develop *CFHB Live*²⁶, an online system that uses series and continued fraction representations to obtain function values and error bounds with negligible added cost. We are collaborating with the Antwerp group to build an online system that allows users to create their own tables of special function values with an error certification [4] for integration within the NIST Digital Library of Mathematical Functions (DLMF). At NIST we are building the front end user interface to work with a back end computational engine based on the MPIeee library.

During the past few months we have focused on the launch of a prototype system at Antwerp. The top level structure is similar to the DLMF. As shown in Figure 40, the table of contents lists names corresponding to chapters found in the DLMF. After a chapter and function are selected, a user may request a tabulation of function values to user-specified precision, or comparison to user-uploaded function values. Each output line of a tabulation that contains the function value and numbers representing an interval bounding the error. Currently, the output of a comparison shows function values computed by the system alternated with corresponding values from the table of data provided by the user, but discussions are ongoing concerning the best output format. There appears to be a consensus that relative errors should be shown along with some indication of digits that are possibly in error as illus-

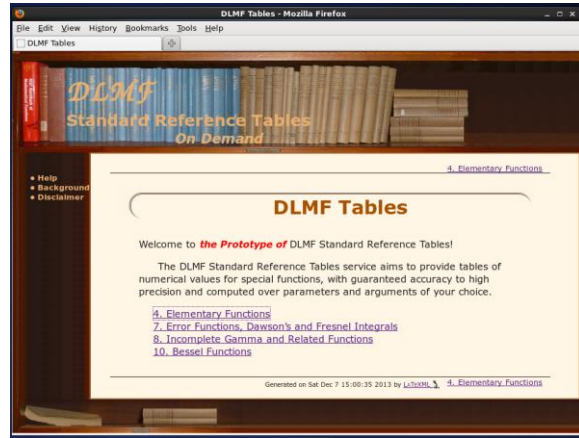


Figure 40. Sample table of contents for DLMF Tables website.

x	exp(x)	Relative Error
0	1.80000 0000 00a02	
0	1.80000 0000	0.0
0	1.80000 0000 00a02	
0	6.39999 9999	1.0 * 10 ⁻⁹
0	1.80000 0000 00a02	
0	1.80000 0000	1.0 * 10 ⁻⁹
0	1.80000 0000 00a02	
0	2.0 * 10 ⁻⁹	2.0 * 10 ⁻⁹
0	1.80000 0000 00a02	
0	1.80000 0000	2.0 * 10 ⁻⁹
1	2.71828 1828 46a03	
1	2.71828 1828	1.7 * 10 ⁻¹⁰
1	2.71828 1828 46a03	
1	2.71828 1828	2.0 * 10 ⁻¹⁰
1	2.71828 1828 46a03	
1	2.71828 1828	5.4 * 10 ⁻¹⁰
6	4.83428 7934 91a05+10 ⁰	
6	4.83428 7935	1.8 * 10 ⁻¹¹
6	4.83428 7934 91a05+10 ⁰	
6	4.83428 7934	2.4 * 10 ⁻¹⁰

Figure 41. Output for comparison of DLMF Tables computations with table of function values submitted by user.

trated in Figure 41. The prototype can be viewed at the University of Antwerp website²⁷.

Several talks were presented about the project this year. Bonita Saunders presented the work at the Mathematical Association of America (MAA) MD-DC-VA Section Meeting at Salisbury University on April 13, 2013. Daniel Lozier presented a minisymposium talk and announced the Antwerp site at the Society for Industrial and Applied Mathematics (SIAM) Annual Meeting in July 2013.

Our current focus includes increasing the number of functions offered, inserting more user documentation, and adding functionality, for example, offering users a choice of rounding modes for tabulations and comparisons. Other issues under discussion include more extensive documentation for experts, integration with the DLMF site, and strenuous testing of inputs to catch potential vulnerabilities. Of course, as some issues are addressed, others are revealed. Consequently, another important job is prioritizing the work so that the NIST site is ready before the end of this fiscal year.

²⁶ <http://www.cfsf.ua.ac.be/>

²⁷ <http://cantlive.ua.ac.be/dlmftables/>

- [1] A. Cuyt, V. B. Petersen, B. Verdonk, H. Waadeland and W. B. Jones, *Handbook of Continued Fractions for Special Functions*. Springer, New York, 2008.
- [2] F. Backeljauw, A Library for Radix-independent Multi-precision IEEE-compliant Floating-point Arithmetic, Technical Report 2009-01, Department of Mathematics and Computer Science, Universiteit Antwerpen, 2009.
- [3] M. Colman, A. Cuyt and J. Van Deun, Validated Computation of Certain Hypergeometric Functions. *ACM Transactions on Mathematical Software* **38:2** (January 2012), Article 11.
- [4] F. Backeljauw, S. Becuwe, A. Cuyt, J. Van Deun, and D. Lozier, Validated Evaluation of Special Mathematical Functions, *Science of Computer Programming* **10** (2013), 1016.

Digital Repository of Mathematical Formulae

Howard S. Cohl

Marjorie A. McClain

Bruce R. Miller

Bonita V. Saunders

Deyan Ginev (Jacobs University Bremen)

Janelle C. Williams (Virginia State University)

<http://drmf.mathweb.org>

The purpose of this project is to create a community-driven digital knowledge base for mathematical formulae, equations, and objects associated with special functions and orthogonal polynomials. The original suggestion for this came from Dmitry Karp in an issue of *OPSF-Net* [1], with follow-up comments by Daniel Lozier [2] and Tom Koornwinder [3, 4]. The project has been ongoing since April 2013, and had a first aim of creating a proof-of-concept deployment. A demonstration will then be presented to the special functions and orthogonal polynomials mathematical community for a first round of feedback. We refer to our deployment, built with the publishing platform used by Wikipedia, namely MediaWiki, as the Digital Repository of Mathematical Formulae (DRMF).

The DRMF is focused on the needs of mathematicians performing research in the field of special functions who wish to (a) disseminate recent research results, and (b) interact with other researchers interested in these results. (In the field of special functions, new results are most often embodied in mathematical formulae.) We also hope that the DRMF will serve as a laboratory providing insight on successfully developing and curating such a resource.

On the technical front, we have built on the experience of the DLMF project²⁸ [5], as well as the

Planetary and MediaWiki publishing platforms. Each feature of the publishing process is modelled as a separate general-purpose MediaWiki extension, and published on GitHub for redistribution. The first demonstration provides experimental extensions for (1) formula interactivity, (2) formula pages, (3) centralized bibliography and (4) mathematical search. At its foundation, DRMF shares the core technologies of the DLMF, based on community-recognized open standards (TeX, HTML+MathML), as integrated by the LaTeXML converter. We incorporate some of the high-quality components used in Planetary (the JOBAD interactivity framework), as well as those designed for MediaWiki (such as the MathSearch and Math extensions). Examples of formula interactivity include:

- a clipboard for mathematics, allowing easy copy/paste of a formula's source, presentation or content MathML representations;
- on-demand summary of constraints and substitutions applicable to a formula;
- on-demand consulting with external web services (e.g., Wolfram Alpha) and local computer algebra systems (e.g., Mathematica, Maple).

The DRMF's first vision of a repository for mathematical formulas is to treat any notable expression as a primary object of interest, describing it in its own "formula page." See Figure 42. Currently, formula pages contain a description of the formula itself, open section for proofs, bibliographic citations, a glossary of special DLMF symbols used in the formula and a link to the formula in the DLMF, whenever applicable. Optionally, one may also enter relevant constraints, substitutions, notes, the formula name, as well as links to formula generalizations and specializations. For each formula page there is a corresponding talk page where discussions about the formula and its page may take place. We are currently developing a strategy for handling the insertion of formula errata.

We are also exploring a variety of search strategies within our MediaWiki deployment. A key asset in our development of search capabilities is the use of DLMF macros in writing the TeX markup of formulas. LaTeXML (see page 71) uniquely translates the macros for specific special functions, orthogonal polynomials and general mathematical objects into Content MathML symbols, which in turn fuel structural search engines, such as MathWebSearch, to return results with very high accuracy.

Next, we present an early overview of the shortlisted resources which we plan to incorporate. We have been given permission to seed the DRMF with data from the NIST Digital Library of Mathematical Functions; Koekoek, Lesky and Swarttouw's (KLS) book *Hypergeometric Orthogonal Polynomials and*

²⁸ <http://dlmf.nist.gov/>

HowardCohl [Talk](#) [Preferences](#) [Watchlist](#) [Contributions](#) [Log out](#)

Page **Discussion** Read [Edit](#) [View history](#)

Formula:DLMF:25.4+E5

<< [Formula:DLMF:25.4+E4](#) formula in list-of-formulas page [Formula:DLMF:25.5+E11](#) >>

$$(-1)^k \zeta^r(k)(1-s) = \frac{2}{(2\pi)^s} \sum_{m=0}^k \sum_{r=0}^m \binom{k}{m} \binom{m}{r} \left(\Re(c^{k-m}) \cos\left(\frac{1}{2}\pi s\right) + \Im(c^{k-m}) \sin\left(\frac{1}{2}\pi s\right) \right) \Gamma^{(r)}(s) \zeta^{(m-r)}(s)$$

Contents [\[hide\]](#)

- 1 [Substitution\(s\)](#)
- 2 [Constraint\(s\)](#)
- 3 [Proof](#)
- 4 [Symbols List](#)
- 5 [Bibliography](#)
- 6 [URL links](#)

Substitution(s) [\[edit\]](#)

$c = -\ln(2\pi) - \frac{1}{2}\pi i$

Constraint(s) [\[edit\]](#)

$s \neq 0, 1, k = 1, 2, 3, \dots$

Proof [\[edit\]](#)

We ask users to provide proof(s), reference(s) to proof(s), or further clarification on the proof(s) in this space.

Symbols List [\[edit\]](#)

(-1) : $(-1) = \text{\opminus}$: <http://dlmf.nist.gov/5.7.E7> [↗](#)

ζ : Riemann zeta function : <http://dlmf.nist.gov/25.2#E1> [↗](#)

π : the ratio of a circle's circumference to its diameter : <http://dlmf.nist.gov/5.19.E4> [↗](#)

$\binom{a}{b}$: binomial coefficient : <http://dlmf.nist.gov/1.2#E1> <http://dlmf.nist.gov/26.3#SS1.p1> [↗](#)

$\Re a$: real part : <http://dlmf.nist.gov/1.9#E2> [↗](#)

cos : cosine function : <http://dlmf.nist.gov/4.14#E2> [↗](#)

$\Im a$: imaginary part : <http://dlmf.nist.gov/1.9#E2> [↗](#)

sin : sine function : <http://dlmf.nist.gov/4.14#E1> [↗](#)

Γ : Euler's gamma function : <http://dlmf.nist.gov/5.2#E1> [↗](#)

ln : principal branch of logarithm function : <http://dlmf.nist.gov/4.2#E2> [↗](#)

i : imaginary unit : <http://dlmf.nist.gov/1.9.i> [↗](#)

Bibliography [\[edit\]](#)

Equation (5), Section 25.4 of **DLMF**.

URL links [\[edit\]](#)

Formula link in **DLMF** [↗](http://DLMF.NIST.GOV/25.4#E5): [HTTP://DLMF.NIST.GOV/25.4#E5](http://DLMF.NIST.GOV/25.4#E5) [↗](#)

<< [Formula:DLMF:25.4+E4](#) formula in list-of-formulas page [Formula:DLMF:25.5+E11](#) >>

Figure 42. Sample DRMF formula page.

Their q-Analogues [6], as well as the Bateman Manuscript Project (BMP) [7, 8].

We are in active communication with other publishers to get permission for other proven sources of mathematical formulae. Our current focus is on seeding the DRMF with DLMF data, and we have completed this for DLMF Chapter 25 on Zeta and Re-

lated Functions. Future near-term efforts will focus on seeding the rest of the DLMF data as well as the KLS data with DLMF macros incorporated. Efforts to upload BMP data will rely on mathematical optical character recognition software to produce LaTeX source for these formulae, and this effort is currently under consideration.

- [1] D. Karp, Knowledge Base of Formulas, *OP-SF NET* **18:4** (2011), Topic 5.
- [2] D. Lozier, Comment 1 on Dmitry Karp's Proposal, *OP-SF NET* **18:4** (2011), Topic 6.
- [3] T. Koorwinder, Comment 2 on Dmitry Karp's proposal, *OP-SF NET* **18:4** (2011), Topic 7.
- [4] T. Koorwinder, Additions to formulas in Koekoek-Lesky-Swartz, *OP-SF NET* **18:6** (2011), Topic 3.
- [5] F. W. J. Olver, D. W. Lozier, R. F. Boisvert and C. W. Clark, *The NIST Digital Library of Mathematical Functions*, Cambridge University Press, 2010.
- [6] R. Koekoek, P. A. Lesky and R. F. Swartz, *Hypergeometric Orthogonal Polynomials and their q -Analogues*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2010.
- [7] A. Erdélyi, W. Magnus, F. Oberhettinger and F. G. Tricomi, *Higher Transcendental Functions*, Vols. I, II, III, Robert E. Krieger Publishing Co. Inc., Melbourne, FL, 1981.
- [8] A. Erdélyi, W. Magnus, F. Oberhettinger and F. G. Tricomi, *Tables of Integral Transforms*, Vols. I and II, Robert E. Krieger Publishing Co. Inc., Melbourne, FL, 1954.

Eigenfunction Expansions for Special Functions and Orthogonal Polynomials

Howard S. Cohl

Hans Volkmer (University of Wisconsin-Milwaukee)

Roberto S. Costas-Santos (University of Alcalá)

Rebekah M. Wheatley (Johns Hopkins University)

Michael A. Baeder (Harvey Mudd College)

Connor MacKenzie (Westminster College)

Philbert Hwang (Poolesville High School)

The concept of a function expresses the idea that one quantity (the input) completely determines another quantity (the output). Our research concerns special functions and orthogonal polynomials. A special function is a function that has appeared in the mathematical sciences so often that it has been given a name. Green's functions (named after the British mathematician George Green, who first developed the concept in the 1830s) describe the influence of natural phenomena such as electromagnetism, gravity, heat and waves. For example, in electrostatics, a Green's function describes the influence of a point charge, called the source, over all of space. The inputs for Green's functions are all of space (with the exception of a singular region), and the output is the "force" exerted from the point throughout space. Green's functions are fundamental to the study of partial differential equations and are powerful in that they provide a mechanism for obtaining their solutions.

We study the properties of Green's functions in spaces which are curved, and in particular, those spaces which locally look the same in every direction, i.e., those that are isotropic. Orthogonal polynomials and the special functions associated with them occupy a natural location in the study of these spaces. We focus on their behavior. Such a study is fundamental to the mathematical understanding of the universe, which as Einstein showed is curved. In particular, we compute eigenfunction expansions for fundamental solutions of multi-dimensional linear elliptic partial differential equations in separable coordinate systems on highly symmetric Riemannian manifolds. These iterated expansions are computed in the natural eigenfunctions produced by the method of separation of variables for elliptic partial differential equations on these manifolds. These iterated expansions are often connected by addition theorems to simpler expansions in fewer discrete and continuous eigenmode variables. We utilize classical analysis on these manifolds in order to obtain new special addition theorems that identify fundamental expansions through specialization and generalization in a geometrical context.

In Euclidean space, fundamental solution expansions can be given in terms of the harmonics expressed in separable coordinate systems. With H. Volkmer, we have an ongoing investigation of these expansions. It is our goal to develop eigenfunction expansions for a fundamental solution of Laplace's equation in three-dimensions in parabolic cylinder, elliptic cylinder, rotationally-invariant cyclidic (fourth order), asymmetric quadric (second order) and asymmetric cyclidic coordinate systems. In connection with this effort, in [1], we compute new definite integrals using orthogonality and integral transforms. These integrals originate from eigenfunction expansions for a fundamental solution of Laplace's equation in three-dimensional Euclidean space in separable, rotationally-invariant coordinate systems. These expansions had been previously computed in [2] and an erratum [3] has been recently published. In [4], we analyzed summation and integration expansions for a fundamental solution of Laplace's equation in three-dimensional Euclidean space in parabolic cylinder and elliptic cylinder coordinates. These expansions are given in terms of parabolic cylinder functions and Mathieu functions, the special functions which arise in these separable coordinate systems for Laplace's equation. In [5] (see also [6]), we performed a global analysis of solutions for Laplace's equation on three dimensional Euclidean space in one of the most general orthogonal asymmetric confocal cyclidic coordinate systems which admit solutions through separation of variables. We refer to this coordinate system as five-cyclidic coordinates since the coordinate surfaces are given by two cyclides of genus zero which represent the inversion at the unit sphere of each other, a cyclide of genus one, and two disconnected cyclides

of genus zero. This coordinate system is obtained by stereographic projection of spherico-conal coordinates on four-dimensional Euclidean space. The harmonics in this coordinate system are given by products of solutions of second-order Fuchsian ordinary differential equations with five elementary singularities. The Dirichlet problem for the global harmonics in this coordinate system is solved using multiparameter spectral theory in the regions bounded by the asymmetric confocal cyclidic coordinate surfaces. H. Volkmer and H. Cohl have submitted a second paper on the topic of asymmetric cyclidic harmonics [12]. In this paper we compute external harmonics for the asymmetric cyclidic separable harmonic five-cyclidic coordinate system, as well as expansions for a fundamental solution of Laplace's equation in these harmonics.

On highly symmetric manifolds, fundamental solution expansions are often given in terms of angular harmonics which are represented in terms of Fourier, Gegenbauer, and Jacobi polynomials. In practice, these expansions are often expressible using generating functions for these orthogonal polynomials. We have developed a technique for generalizing generating functions for hypergeometric orthogonal polynomials which has been useful in developing fundamental solution expansions. In [7], a generalization of the generating function for Gegenbauer polynomials is derived which allows one to expand this generating function in terms of Gegenbauer polynomials with arbitrary order. This Gegenbauer polynomial expansion allows one to expand powers of the distance between two points in d -dimensional Euclidean space in Vilenkin's polyspherical coordinates. In [8], we describe two methods for computing azimuthal Fourier expansions for a logarithmic fundamental solution of the polyharmonic equation in d -dimensional Euclidean space. In [9], we compute a generalization of the generating function for Gegenbauer polynomials extended to Jacobi polynomials. The expansion with Chebyshev polynomials of the first kind is used to compute Fourier expansions for a power-law fundamental solution of the polyharmonic equation in d -dimensional Euclidean space in rotationally-invariant coordinate systems. In [9], addition theorems for the Fourier coefficients of a power-law fundamental solution of the polyharmonic equation in d -dimensional Euclidean space in Vilenkin's polyspherical coordinates are computed. We also develop addition theorems for Fourier coefficients of fundamental solutions for linear elliptic partial differential equations on highly symmetric Riemannian manifolds. With 2013 Summer Undergraduate Research Fellowship (SURF) student, Rebekah Wheatley, we derived Fourier and Gegenbauer expansions for a fundamental solution of Laplace's equation in hyperspherical geometry. Under Cohl's supervision, Wheatley computed Fourier and Gegenbauer expansions and corresponding addition theorems for a

fundamental solution of Laplace's equation in d -dimensional hyperspherical geometry.

Furthermore, we have developed specializations and generalizations of generating functions for orthogonal polynomials in the Askey scheme for generalized hypergeometric orthogonal polynomials. For instance, in [10], we present an interesting extension of the generating function for Gegenbauer polynomials to Jacobi polynomials, and re-expresses Gauss hypergeometric functions in terms of more elementary functions for certain generating functions for classical orthogonal polynomials. We also produce corresponding definite integrals using orthogonality. In [11] (joint with H. Volkmer and 2012 SURF student Connor MacKenzie) we generalize generating functions for hypergeometric orthogonal polynomials, namely Jacobi, Laguerre and Wilson polynomials. These generalizations are determined using connection relations with one free parameter for these hypergeometric orthogonal polynomials. The coefficients of these expansions are given in terms of generalized hypergeometric functions. We then produce corresponding definite integrals using orthogonality. With 2013 SURF student Michael Baeder, we extend the work presented in [11] to other generating functions for hypergeometric orthogonal polynomials, such as Wilson, continuous Hahn, continuous dual Hahn and Meixner-Pollaczek polynomials. We are also extending this investigation to include discrete orthogonal polynomials such as Racah polynomials. Akin to [11], with 2013 Summer High School Internship Program (SHIP) student Philbert Hwang and with Roberto Costas-Santos, we compute generalizations of generating functions for basic hypergeometric orthogonal polynomials in the q -Askey scheme.

- [1] H. S. Cohl and H. Volkmer, Definite Integrals using Orthogonality and Integral Transforms, *Symmetry, Integrability and Geometry: Methods and Applications* **8** (2012), 077.
- [2] H. S. Cohl, J. E. Tohline, A. R. P. Rau and H. M. Srivastava, Developments in Determining the Gravitational Potential using Toroidal Functions, *Astronomische Nachrichten* **321:5/6** (2000), 363-372.
- [3] H. S. Cohl, Erratum: "Developments in Determining the Gravitational Potential using Toroidal Functions," *Astronomische Nachrichten* **333:8** (2012), 784-785.
- [4] H. S. Cohl and H. Volkmer, Eigenfunction Expansions for a Fundamental Solution of Laplace's Equation on \mathbf{R}^3 in Parabolic and Elliptic Cylinder Coordinates, *Journal of Physics A: Mathematical and Theoretical* **45:35** (2012), 355204.
- [5] H. S. Cohl and H. Volkmer, Separation of Variables in an Asymmetric Cyclidic Coordinate System, *Journal of Mathematical Physics* **54:6** (2013), 06351.
- [6] H. S. Cohl and H. Volkmer, Publisher's Note: "Separation of Variables in an Asymmetric Cyclidic Coordinate System," *Journal of Mathematical Physics* **54:7** (2013), 079904.

- [7] H. S. Cohl, On a Generalization of the Generating Function for Gegenbauer Polynomials, *Integral Transforms and Special Functions* **24:10** (2013), 807-816.
- [8] H. S. Cohl, Fourier Expansions for Logarithmic Fundamental Solutions of the Polyharmonic Equation, *Journal of Classical Analysis* **2:2** (2013), 107-127.
- [9] H. S. Cohl, Fourier, Gegenbauer and Jacobi Expansions for a Power-law Fundamental Solution of the Polyharmonic Equation and Polyspherical Addition Theorems, *Symmetry, Integrability and Geometry: Methods and Applications* **9** (2013), 042.
- [10] H. S. Cohl and C. MacKenzie, Generalizations and Specializations of Generating Functions for Jacobi, Gegenbauer, Chebyshev and Legendre Polynomials with Definite Integrals, *Journal of Classical Analysis* **31** (2013), 17-33.
- [11] H. S. Cohl, C. MacKenzie and H. Volkmer, Generalizations of Generating Functions for Hypergeometric Orthogonal Polynomials with Definite Integrals, *Journal of Mathematical Analysis and Applications* **407:2** (2013), 211-225.
- [12] H. S. Cohl and H. Volkmer, Expansions for a Fundamental Solution of Laplace's Equation on \mathbf{R}^3 in Five-cyclidic Harmonics, in review.

Quantum Information

An emerging discipline at the intersection of physics and computer science, quantum information science (QIS) is likely to revolutionize science and technology in the same way that lasers, electronics, and computers did in the 20th century. By encoding information into quantum states of matter, one can, in theory, exploit the seemingly strange and counter-intuitive behavior of quantum systems to enable phenomenal increases in information storage and processing capability, as well as communication channels with extremely high levels of security. Although many of the necessary physical manipulations of quantum states have been demonstrated experimentally, scaling these up to enable fully capable quantum computers remains a grand challenge. We are engaged in (a) theoretical studies to understand the true power of quantum computing, (b) collaborative efforts with the multi-laboratory experimental quantum science program at NIST to characterize and benchmark specific physical implementations of quantum information processing, and (c) the development and assessment of technologies for quantum communication.

Single Photon Conversion Technology: Research to Commercialization

*Xiao Tang
Lijun Ma
Paulina Kuo
Oliver Slattery
Yong-Su Kim
Alan Mink
Barry Hershman
Joshua Bienfang (NIST PML)
Martin Fejer (Stanford University)
Jason Pelc (Stanford University)
Li Yan (University of Maryland Baltimore County)*

See feature article, page 22.

Quantum Information Science

*Scott Glancy
Emanuel Knill
Adam Keith
Adam Meier
Jim van Meter
Mike Mullan
Yanbao Zhang
Kevin Coakley (NIST ITL)
Sae Woo Nam (NIST PML)
B. Eastin (Northrop Grumman)
E. Cobanera (Indiana University)
G. Ortiz (Indiana University)*

The traditional information units of classical computing are 0/1-valued bits, which may be realized as distinguishable states of physical systems. Quantum information science investigates the properties and applications of quantum bits. Formally, quantum bits have pure states defined as superpositions of two dis-

tinguishable states. Quantum bits promise to be powerful information processing units whose potential is realized when they are coupled by means of quantum gates, which generalize classical circuit elements. Applications include efficient algorithms for factoring integers and for physics simulation, protocols for secure communication, and significantly improved measurement precision. In addition, there is the potential for illuminating the foundations of physics, in particular the universality of quantum mechanics and field theory. In the last few years, there has been tremendous experimental progress demonstrating long-lived quantum bits in diverse systems, including individually trapped atoms, superconducting circuit elements and various other solid state devices. Thus, we currently expect that quantum information processing will eventually be realized on large scales.

Our work in quantum information science aims to contribute to our understanding of the power and limitations of quantum physics as it relates to information extraction and processing. In this spirit, we investigate a broad range of subjects. In the current reporting period, we determined effective analysis methods for certifying that experiments violate classicality assumptions, we obtained new criteria for showing that time-tagged detections violate such assumptions, and we initiated an investigation of quantum measurements of properties of curved space-time.

The principle of local realism (LR) asserts that states of spatially separate systems can be described as probability distributions over states where each system is in a definite state. Quantum mechanics violates this principle. Experimental demonstrations of this violation usually involve measuring a so-called Bell quantity and showing that the measured value violates a bound satisfied by LR. While violations have been found in many experiments, these experiments have so far been subject to various loopholes. That is, they require additional, unwanted assumptions to conclude that local realism fails. We are involved in experiments that aim to “close” these loopholes and apply the prop-

erties of the violating quantum systems to device-independent random number generation, a protocol enabled by quantum mechanics. We therefore improved the analysis of LR violation so that an unambiguous statement of statistical significance is obtained. Our method is highly robust in that it is compatible with arbitrary strategies for stopping the experiment and can be used to compare the violation between disparate experiments. For our applications, it provides a strong certificate of performance, a necessity for protocols such as random number generation. This research is the main contribution of Yanbao Zhang's PhD thesis [2], completed this year. Yanbao is continuing to work in this area at the Institute for Quantum Computing in Waterloo, Canada.

Recent experiments to close the loopholes when demonstrating the failure of LR involved observations consisting of series of time tagged detections of photon pairs at various measurement settings. Traditional Bell inequalities work only for one photon pair at a time, requiring that each photon pair can be unambiguously identified in the data. Because of jitter in the recorded detection times and high rates of pair emission, this identification is not assured. As a result, the Bell inequalities can be violated by an LR source taking advantage of this effect. We developed a general theory of Bell quantities and inequalities for time tag sequences [3], integrated it with the analysis methods of the previous paragraph, and applied it successfully to experimental data from two external groups.

Looking further ahead, we are interested in how one can best measure properties of and discover new features of any quantum system. It is in this spirit that we have contributed to the study of non-abelian dualities for better understanding unconventional condensed matter systems [1].

While quantum effects are actively exploited for extremely precise measurements of time (atomic clocks) and space (interferometry for gravitational wave measurements), how properties of quantum field theory in space-time will affect these measurements is not well explored. We are investigating how these properties result in deviations from expectations based on non-relativistic quantum mechanics and at what level of precision these deviations become significant. Our initial focus is on Heisenberg-uncertainty-like limitations on measurements of the space-time metric. There is not yet an agreement on the best framework for analyzing such limitations. So far we have found that with respect to local quantum field theory on curved space times, there are issues with several existing arguments, including the lack of coordinate independence.

- [1] E. Cobanera, G. Ortiz and E. Knill, The Non-Abelian Duality Problem, in review.
- [2] Y. Zhang, *Analysis of Tests of Local Realism*, Ph.D. Thesis, University of Colorado, Boulder, 2013.

- [3] Y. Zhang, S. Glancy and E. Knill, Efficient Quantification of Experimental Evidence Against Local Realism, *Physical Review A* **8** (2013), 052119.

Quantum Computing Benchmarks

Emanuel Knill

Adam Meier

Michael Mullan

Dietrich Leibfried (NIST PL)

David Wineland (NIST PL)

David Pappas (NIST PL)

While the potential benefits of quantum information processing are tremendous, there are significant obstacles in realizing these benefits. Perhaps the most challenging obstacles are to experimentally construct multi-qubit systems whose quantum states are both stable and robustly manipulatable by quantum gates. One reason the two requirements are difficult to meet is that stability requires good isolation from the environment, but manipulatability involves interaction with an external controller. There is a proliferation of experimental systems that aim to meet these requirements with a few qubits and that hope to eventually scale up to many qubits. To evaluate such systems without regard to experimental details, we develop benchmarks, which are standardized processes and measurements that quantify the quality and scale of the experimental quantum system for information processing.

Over the past few years we have developed and implemented a randomized benchmarking strategy that has been widely adopted. At NIST it has been implemented with trapped ion-qubits. The benchmarking procedures used and experimental analysis applied were the main contributions of Adam Meier's PhD thesis [1], completed this year. Adam is continuing this work at the Georgia Tech Institute.

A simple strategy for testing an experimental two-qubit gate is to prepare a maximally entangled state and measure each qubit in various bases. The fidelity of the state measurement can then be inferred from the data. This strategy has been used for characterizations of spin-spin interactions in ion-trap experiments at NIST [3]. A recent version of this experiment brought to light several issues with this technique. The first is that the measurements need to be calibrated using similar measurements on known states. The instruments must be stable during the calibration and the subsequent measurements for this to work. Since perfect stability is unachievable, this requires additional tests to bound the contributions due to instability. At least one data set thought to be good turned out to suffer from this issue. The quality of the calibration becomes particularly important as the precision of the fidelity measurement improves or the fidelity approaches its maximum value

of 1. For example, at the moment it is not clear whether we could confidently claim fidelity better than (say) 0.995 in such an experiment. Traditionally, the data of the ion-trap experiments involve decomposing detection-count histograms as a mixture of reference histograms, where the latter are calibrated beforehand. Our analysis now bypasses the need for a full determination of reference histograms by using linear functionals of histograms to estimate the fundamental quantities from which the fidelity can be computed. We hope to integrate the new techniques into the control and data acquisition system in NIST's ion-trap labs.

A general theme of this project is to develop better measurement strategies involving general quantum systems. In this spirit, we are formulating the theory and implementing algorithms and simulations for actively estimating the current time with passive atomic clocks, particularly the so-called quantum logic clocks. This work constitutes the PhD Thesis of Mike Mullan [2], completed this year, and is being developed further by Adam Keith. So far we have successfully demonstrated improvements in timekeeping with simulated clocks subject to memory-less local oscillator noise. A goal is to demonstrate our strategies on an experimental system such as trapped beryllium ions.

- [1] A. M. Meier, *Randomized Benchmarking of Clifford Operators*, PhD Thesis, University of Colorado, Boulder, 2013.
- [2] M. Mullan, *Quantum Algorithms for Atomic Clocks*, PhD Thesis, University of Colorado, Boulder, 2013.
- [3] A. C. Wilson, Y. Colombe, K. R. Brown, E. Knill, D. Leibfried and D. J. Wineland, Entangling Spin-Spin Interactions of Ions in Individually Controlled Potential Wells, in review.

Quantum State Estimation Theory and Experiment

Scott Glancy

Emanuel Knill

Konrad Lehnert (NIST PML)

Will Kindel (University of Colorado)

Hsiang-Sheng Ku (University of Colorado)

Many emerging technologies will exploit quantum mechanical effects to enhance metrology, computation, and communication. Developing these technologies requires improved methods to measure the state of quantum systems. Quantum state estimation is a statistical problem of estimating an underlying quantum state using a collection of measurements made on independently prepared copies of the state. Accurate quantum state estimation allows experimentalists to answer the questions “What quantum state does my device prepare?” and “How certain am I that it has prepared that state?”

Full quantum state estimation can be a demanding task, requiring a large number of different measurements to be performed on (independently prepared copies) of the quantum state and requiring large amounts of computation to estimate the state. One method for reducing these costs is to exploit pre-existing knowledge about the state being measured. For example, the state could be restricted to a smaller sub-set of all quantum states, such as those states that have Gaussian probability distributions for measurement results. ACMD developed an algorithm for estimating these Gaussian states that is orders of magnitude faster than full quantum state estimation and can be applied to data sets that are much too large to be analyzed with full quantum state estimation. ACMD's new algorithm will be useful to many experiments on quantum optics and nano-mechanical resonators.

ACMD continues the collaboration with the JILA laboratory of Konrad Lehnert through the Defense Advanced Research Projects Agency (DARPA) project titled “Analog Quantum Integrated Circuits.” The goal of this project is to create entangled states in superconducting microwave circuits and to use that entanglement for quantum teleportation. In 2013 the laboratory prepared an entangled state of quantum microwaves. ACMD developed methods to calibrate the measurements, analyze the entangled state using a phenomenological model and using Gaussian state estimation, and quantify the amount of entanglement. After demonstrating entanglement in this system, the experiment will progress to achieving the increased measurement efficiency required for quantum teleportation and optimizing the teleportation protocols for this system.

Random Number Generation based on Bell Inequality Violation

Scott Glancy

Stephen Jordan

Emanuel Knill

Paulina Kuo

Yi-Kai Liu

Alan Mink

Xiao Tang

Lawrence Bassham (NIST ITL)

Joshua Bienfang (NIST PML)

Michaela Iorga (NIST ITL)

Alan Migdall (NIST PML)

Sae Woo Nam (NIST PML)

Rene Peralta (NIST ITL)

Andrea Rommal (Muhlenburg College)

Andrew Rukhin (NIST ITL)

Random number generation is a key step in almost all cryptographic protocols. For cryptographic applications one needs to know that the random numbers used could not have been known prior to their generation. There are no empirical tests on classical data that can certify this. However, using counterintuitive aspects of quantum mechanics, it is possible to empirically verify the generation of random numbers that could not have been known prior to their measurement without violating fundamental laws of physics. This can be achieved using modern variants of Einstein's "spooky action at a distance" thought experiment, known as Bell tests. Recently, advances in quantum optics technology have moved these tests from the realm of thought experiments into the laboratory. A current NIST Innovations in Measurement Science project involving several members of ACMD seeks to implement an optical Bell experiment and use it to produce random numbers certifiably secure for use in cryptographic applications.

Despite technological advancements, implementing Bell tests remains challenging. Work has been ongoing at NIST to integrate fast, highly-efficient photon detectors, high-speed optical switching, and low-loss photon transmission into a Bell experiment whose data analysis can be carried out with minimal assumptions. Within ACMD, efforts have focused on developing tools for data analysis, analyzing alternative architectures for the experiment, and developing hardware and software infrastructure for the information-theoretic and cryptographic aspects of the project, such as post-processing algorithms to evaluate and extract the attained randomness.

On July 21-26, 2013 several members of ACMD met in Boulder for an intensive workshop on Bell-based randomness. Several protocols for processing random numbers using Bell experiments have been proposed in the quantum information theory literature. All of them require some initial seed of random numbers. Randomness expansion protocols start with a small seed and expand it via Bell experiments into a larger supply of random bits. Randomness amplification protocols start with an imperfect private seed and amplify it into an almost perfectly private supply of random numbers. A significant outcome of the workshop was a survey of the theoretical protocols and the corresponding hardware requirements for each.

The Bell experiment needs several additional ingredients to become a useful cryptographic resource. These include: a source of random numbers to use as the initial seed, software for analyzing the outcomes of the experiment to certify the presence of fresh randomness, software for distilling the data produced by the experiment into nearly-uniformly-random strings of bits, and technology to publish these strings over the Internet. Over the past year, ACMD has made progress in the development of each of these.

A prototype "randomness beacon" serving time stamped, digitally-signed random bit strings over the

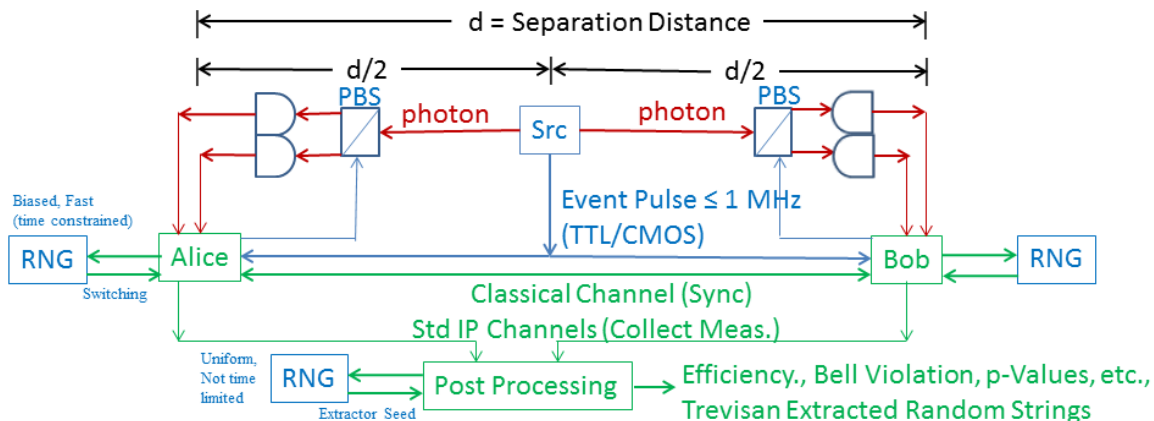


Figure 43. Architecture of Bell experiment random number generator implementation.

internet, developed by the ITL Computer Security Division, is currently operational²⁹. The prototype beacon uses a conventional hardware random number source not based on Bell experiments. Although the unpredictability of these random numbers is not certifiable by direct appeal to the laws of physics, the beacon can serve as a testbed for the various beacon-based cryptographic protocols for e-commerce and privacy protection that have been proposed in the cryptographic theory literature.

ACMD has developed an architectural model for Bell based randomness, as shown in Figure 43. Plans are to implement that model using field programmable gate arrays (FPGAs) at Bob and Alice to capture and timestamp detector events, as well as to generate supplemental supplies of random numbers for measurement basis selection and Trevisan extractor seeds.

Many Bell experiments generate entangled photon pairs randomly in time, and the detectors used to measure the photons suffer from timing jitter. These effects can create confusion in the “time-tag” measurement record that could allow a hacker to secretly control the random numbers output by the experiment. ACMD has developed new analysis tools for these experiments that can detect any such hacking attempt. After certifying the impossibility of local hidden variable models for the output data, the next step is to distill the output data into a string of almost perfectly uniform random bits. This is achieved by a software tool called a randomness extractor. We have now implemented, tested, and debugged a version of the Trevisan randomness extractor and have additionally identified theoretical improvements to that extractor.

Although Bell experiments expand or amplify initial supplies of random numbers, it is of course desirable for these initial supplies to be of as high a quality as possible. Ideally, the initial random numbers should be unpredictable and produced at high rate and with low latency. Several methods for generating the initial supply of random numbers have been investigated, and one has now been implemented, specifically a random number generator based on a chaotic analog circuit implemented within an FPGA.

Tamper-Resistant Cryptographic Devices based on Quantum Mechanics

Yi-Kai Liu

In recent years there has been growing interest in building tamper-resistant cryptographic devices, for applications such as software copy-protection and digital rights management. For example, many video game consoles use tamper-resistant chips to prevent unauthorized software from being loaded onto the system. Tamper-resistant chips can also be useful in preventing side-channel attacks, where an adversary tries to gain extra information about a computation by measuring physical characteristics of the hardware, such as timing and power consumption.

Can one make use of quantum mechanics to build better tamper-resistant cryptographic devices? One may hope that this is possible, because information behaves in surprising ways when it is encoded into the state of a quantum mechanical object. For instance, an unknown quantum state cannot be copied perfectly, and most measurements of the state will damage it. On the other hand, entangled quantum states can exhibit correlations that are impossible in a classical world, and can be used to perform novel tasks such as device-independent quantum key distribution.

We are developing a quantum-based approach to construct an important class of tamper-resistant devices called “one-time memories.” Roughly speaking, a one-time memory is a device that stores two messages, in such a way that a user can retrieve either the first message or the second message, but not both. One-time memories are relatively simple to construct, yet they are known to be extremely powerful. In particular, they can be used to build “one-time programs,” which have the following behavior: a user can run the program exactly once, but the program hides its internal state (as if it were an oracle or “black box”), and after one execution the program becomes unusable (as if it had “self-destructed”).

We find that one-time memories *cannot* exist in a world that is fully classical or fully quantum; but, surprisingly, one-time memories *can* be built in a world that is *partly* quantum. More precisely, one-time memories can be built from “isolated qubits,” which are a quantum resource (qubits that can be prepared and measured in superposition states) combined with a classical restriction (that it is impossible to perform entangling operations on pairs of qubits). This is interesting from a theoretical perspective, as it touches on fundamental questions in quantum information theory, concerning the power of local operations and classical communication, and the phenomenon of “nonlocality without entanglement.” It is also interesting from a

²⁹ <https://beacon.nist.gov/home>

practical perspective, as there are plausible experimental realizations of isolated qubits, using nuclear spins in solid-state materials.

The next step will be to improve the security and efficiency of our constructions for one-time memories. In particular, our present constructions have a number of drawbacks: they are purely information-theoretic, not computationally efficient, and the security guarantees we have shown are not strong enough to support the construction of one-time programs. We believe that improvement in all of these areas should be possible.

- [1] Y.-K. Liu, Building One-Time Memories from Isolated Qubits, *Proceedings of ITCS 2014: Innovations in Theoretical Computer Science*, to appear.

Post-Quantum Cryptography

Stephen Jordan

Yi-Kai Liu

Lily Chen (NIST ITL)

Dustin Moody (NIST ITL)

Rene Peralta (NIST ITL)

Ray Perlner (NIST ITL)

Daniel Smith-Tone (NIST ITL)

The development of quantum computers creates new challenges and new opportunities for cryptography. If large-scale quantum computers are ever built, they would break many of the cryptosystems that are currently used to protect communications on the Internet, such as RSA, Diffie-Hellman and elliptic curve cryptosystems. Thus, there is now considerable interest in designing so-called “post-quantum” cryptosystems that would be secure against quantum attacks. We have been investigating this area, with a view to developing future standards for public key cryptography.

Some proposals for quantum-resistant cryptosystems include lattice-based cryptosystems (such as NTRU), code-based cryptosystems (such as McEliece), multivariate cryptosystems (such as HFE and unbalanced oil-vinegar), hash-based signatures (such as Merkle trees), and key exchange protocols based on elliptic curve isogenies. However, all of these proposals face significant open questions regarding their security and practical feasibility.

In the past year we have examined these issues in greater detail. In particular, we have compiled a list of evaluation criteria for post-quantum encryption and signature schemes, covering issues such as security, performance and compatibility with existing applications. We have also studied the feasibility of integrating these post-quantum cryptographic primitives into higher-level protocols such as TLS (Transport Layer Security) and IPSec (Internet Protocol Security); this indicates a potential need for post-

quantum key exchange protocols, in addition to encryption and signature schemes.

We have surveyed a number of different approaches to evaluating the security of post-quantum cryptosystems, including empirical studies of the performance of known cryptanalytic attacks, proofs of security based on conjectures in computational complexity theory, and formal analysis that upper-bounds the power of certain common classes of attacks. In particular, we have surveyed recent work on lattice basis reduction, quantum algorithms for finding isogenies of elliptic curves, Grobner basis attacks on code-based cryptosystems, and differential attacks on multivariate cryptosystems. Finally, we have been keeping up with recent progress in lattice-based signature schemes.

We have discussed some research questions with technical staff from the Trusted Systems Research Group at the National Security Agency. We also participated in a conference on Quantum-Safe Cryptography organized by the European Telecommunications Standards Institute (ETSI), where we presented talks on “Practical Impacts of Quantum Computing” and “Evaluating the Security of Post-Quantum Cryptosystems.”

High-Speed Low Density Parity Codes for Quantum Key Distribution

Alan Mink

Anastase Nakassis (NIST ITL)

Quantum information science incorporates quantum mechanics into information technology. It is an emerging field thought to have the potential to cause revolutionary advances. One promising early area is quantum cryptography, specifically Quantum Key Distribution (QKD), which is a protocol that uses a pair of unsecured communication channels, a quantum channel and a classical channel, to establish a shared secret between two parties, Alice and Bob. This shared secret is then used to encrypt messages between Bob and Alice. QKD has been proven information theoretically secure, unlike classical key distribution that relies on computational complexity.

There are four stages to the QKD protocol. The first stage involves quantum mechanics, while the other three use classical processing. Stage 1 is the transmission of randomly encoded single photons over a lossy quantum channel to be measured by Bob. Stage 2 is where Alice and Bob exchange information over the classical channel to “sift” their bit sequences to achieve a common sequence. But since that sequence may have errors, in Stage 3 Alice and Bob exchange information over the classical channel to correct errors in their bit

sequences without exposing the value of their bits. Stage 4 is where Alice and Bob amplify the privacy of their now identical bit sequences through the application of a hash function to eliminate any leaked information, yielding a smaller set of secret bits between Alice and Bob. The last two stages are referred to as post-processing.

There is a large body of information about error correction (EC) codes, but QKD presents a different environment than conventional communication. For example, expected QKD error rates (1% to 11% vs. 0.1% or below) are higher, error correction information is sent separately over an error free channel, the amount of information that the EC code leaks about the data must be minimized and kept below a given limit to enable the extraction of a secret, and quantum data retransmission is not possible.

Researchers are pursuing the next generation of QKD systems, ones that can attain higher speeds and longer distances. Our focus is on speed; moving from the current Mb/s to the Gb/s secure key generation rate will require highly optimized and parallel implementations of QKD post processing algorithms. One-way EC algorithms, such as low density parity check (LDPC) and Polar codes, tend to be coarse grained computations in that a given data set does not need to communicate until a solution is obtained. Such algorithms are amenable to parallel implementation. Each data set can be assigned to a separate computation engine, which would operate independently in parallel, but each result must be collected sequentially to maintain the required synchronization between Alice and Bob's bits. Also a single communication round trip reduces delays, a benefit as the distance between Alice and Bob increases.

We have shown [1] that bit error estimation can be combined with the EC algorithm to avoid extra communication and time delays and that the size of the data block for EC and privacy amplification doesn't need to be the same. In general, it is advantageous to size those blocks for the specific algorithms, usually EC in smaller blocks, and then combine the data into larger blocks, using actual error rate for privacy amplification.

Although previous QKD implementations have relied heavily on field programmable gate arrays (FPGAs) to attain the Mb/s current operating range, we have found that FPGAs are not suited for Gb/s post proceeding operations. This is mainly due to their relatively limited memory resources. One-way EC algorithms require an order of magnitude more memory than the original class of Cascade EC algorithms, limiting opportunities for parallel instantiation on an FPGA, and thus overall speed-up. Furthermore, speeding-up a given instantiation requires an n-port memory, which allows parallel simultaneous memory accesses to attain higher throughput, which FPGAs have even smaller amounts of. These memories can be

designed into ASICs, and as a result Gb/s LDPC EC has been achieved for 10 Gigabit Ethernet operations. Alternatively, less expensive LDPC implementations on graphical processing units (GPUs) have reported operations in the 100 Mb/s range, and the new generation of GPUs claim to be an order of magnitude faster.

Our experiments [1] have shown that CPU and FPGA implementations of LDPC for QKD can achieve a few Mb/s of throughput, while initial implementations, on an older GPU, has performed an order of magnitude faster. Throughput of LPDC algorithms depend on the data error rate and the proximity to the Shannon limit, thus impacting the amount of entropy one can extract in privacy amplification. We have evaluated the EC performance of our LDPC implementations over the QKD operating range and found that throughput diminishes as the Shannon limit is approached. Our plans are to optimize our GPU implementation to achieve another order of magnitude of performance that could translate to Gb/s throughput on the newer generation of GPUs.

- [1] A. Mink and A. Nakassis, Practical Strategies for QKD Key Production, in Proceedings of the SPIE 8749 (April 2013), Defense Security and Sensing, Baltimore, MD, 840009.

Simulating Quantum Field Theories on Quantum Computers

Stephen Jordan

Keith Lee (University of Waterloo and Perimeter Inst.)

John Preskill (Caltech)

Hari Krovi (BBN Technologies)

Quantum field theories arose as a way to make quantum mechanics compatible with special relativity. Today, they are a central tool in physics, used to describe both the behavior of high energy particles and of condensed-matter systems such as superconductors and semiconductors. In particular, the most fundamental theory of physics to have passed experimental test is the Standard Model of particle physics that describes all known forces except gravity within a unified framework of quantum field theory.

Like all quantum theories, quantum field theories are computationally difficult to simulate because the dimension of the state space scales exponentially with the number of degrees of freedom. Quantum field theories present the additional difficulty that the set of degrees of freedom is formally infinite. It is worth noting that familiar classical field theories such as Maxwell's equations for electromagnetism also suffer from a formally infinite set of degrees of freedom. The standard approach for simulating both quantum and classical field theories is to truncate to a finite set of

degrees of freedom through discretization. However, in the case of quantum field theories there is a surprising and nontrivial interplay between quantum effects and discretization effects known as renormalization.

One of the key challenges in this project is using the theory of renormalization to analyze the errors incurred by discretizing a quantum field theory to make it suitable for simulation on a quantum computer. The simulation of discretized quantum field theories on conventional supercomputers is also a well-studied topic. However, conventional supercomputers are only able to solve what might be termed statics problems in quantum field theory, such as estimating binding energies of nuclei. Dynamics problems, such as simulating relativistic scattering processes as studied in particle colliders, become rapidly intractable for even the most powerful conventional supercomputers as the number of particles increases. For such problems, our analysis shows quantum computers to be capable of achieving exponential speedup over classical computers [1].

In addition to discretization, two further aspects of the simulation problem demanded particular attention. The first is preparation of physically realistic initial states, and the second is simulation of detectors. These tasks unfortunately turn out to be strongly dependent on the details of the underlying quantum field theory.

Our initial work [1] showed how to simulate relativistic scattering of massive bosons. Our recent work has focused on extending our state preparation techniques to handle massive fermions, and to optimizing our techniques for simulating detectors. The ultimate goal is to simulate bosons and fermions in both the massive and massless cases. This would show that the full Standard Model can be efficiently simulated on quantum computers and would imply that, excluding gravity, the known constituents of our universe are not capable of computational power beyond that offered by quantum computers.

Lastly, we are seeking to encode universal quantum computations into idealized particle scattering processes. Such an encoding would imply that if a polynomial-time classical algorithm is ever discovered for simulating particle scattering in quantum field theory, then classical computers could efficiently emulate everything that quantum computers are capable of doing. There is significant evidence (though no mathematical proof) that quantum algorithms are, for certain problems such as integer factorization, exponentially faster than classical algorithms. Thus, our embedding could be thought of as evidence that the problem of simulating particle scattering processes in quantum field theories is in fact exponentially hard for classical computers.

- [1] S. P. Jordan, K. S. M. Lee and J. Preskill, Quantum Algorithms for Quantum Field Theories, *Science* **336** (2012), 1130-1133.

Circuit Obfuscation and Synthesis

Stephen Jordan

Gorjan Alagic (Caltech)

Stacey Jeffery (University of Waterloo)

Aniruddha Bapat (Caltech)

Logic gates, for both classical and quantum computation, obey various identities and can be treated as an algebraic system. Algebraic manipulation of logic circuits has many applications, which include automated synthesis of optimized circuits, testing equivalence of circuits, and obfuscation of circuits. Obfuscation is perhaps the most exotic and least familiar of these applications. Roughly speaking, a circuit obfuscator is an algorithm that applies circuit identities to scramble a circuit, thereby making it difficult to reverse-engineer while preserving its functionality. Aside from its obvious applications to protecting intellectual property, obfuscation is known to be a powerful primitive from which numerous other cryptographic protocols can be constructed.

One way to obfuscate circuits is to reduce them to a canonical form uniquely determined by the circuit's truth table. This erases all information about the circuit's original implementation. This has been achieved for certain limited classes of circuits, but it is provably impossible to reduce general logic circuits to a canonical form in polynomial time. Interestingly, the feasibility of a slight variant of this idea remained an open question until recently. Specifically, motivated by physical considerations including quantum mechanics, a notion of reversible circuits has been introduced, in which no data is ever erased. The problem of reduction to canonical form is significantly different for reversible circuits than for conventional logic circuits. Nevertheless, we recently proved that this is also impossible to achieve by any efficient (i.e., polynomial-time) algorithm [2].

In light of no-go theorems such as the above, one can seek to satisfy weaker, but still useful, security definitions. In a recent breakthrough, Garg et al. have found a polynomial-time algorithm which, under plausible cryptographic assumptions, produces obfuscated circuits such that circuits with the same truth table are not reduced to forms that are identical, but rather are (in a certain precise sense) computationally indistinguishable. Our current work includes the investigation of ways to adapt these new techniques to quantum circuits. We have also proposed an alternative way of weakening the notion of obfuscation, which we call partial-indistinguishability obfuscation [1]. The idea is that by culling the list of circuit identities one can make the reductions to canonical form tractable.

A polynomial-time algorithm is known for reducing words in the braid group to canonical form. Therefore, circuits composed from logic gates that

obey the identities of the braid group generators can be efficiently obfuscated in a way that satisfies our “partial-indistinguishability” definition. Satisfying the identities of the braid group generators may appear to be a rather peculiar property for a set of logic gates to possess. However, in the quantum world this arises quite naturally—the braiding of certain exotic quasiparticles called anyons can achieve a complete set of quantum logic operations. Furthermore, using ideas from quantum physics, classical logic gates satisfying the relations of the braid group generators have also been discovered.

Motivated by applications to circuit obfuscation, we have been investigating more efficient ways to translate circuits into gate-sets that obey the braid group relations. In particular, the best published scheme for braid-based classical computation does not use logic gates acting on bits, but rather on 60-state “dits”. We have reduced this to 44 states. We have also performed computer searches that suggest that classical braid-based computing using dits of 5 states or fewer is impossible. In addition, we have proven that braid-based quantum computation with standard 2-state qubits is impossible.

Aside from obfuscation, one of the main applications of algebraic techniques to circuit design is circuit optimization. There are many metrics that one can seek to optimize. One metric of particular importance in optimizing quantum circuits is the number of qubits used as working memory. Recently, we have discovered a group-theoretic construction showing that a much more general class of quantum circuits can be implemented “in-place” than was known previously. Specifically, other than the input qubits, no additional workspace is needed to implement quantum gates controlled by arbitrary Boolean formulas. The previous best construction achieved this for the special case where the Boolean formula was composed only from logical AND.

- [1] G. Alagic, S. Jeffery and S. P. Jordan, Partial-indistinguishability Obfuscation using Braids, arXiv:1212.6458, December 2012.
- [2] S. P. Jordan, Strong Equivalence of Reversible Circuits is coNP-Complete, arXiv:1307.0836, July 2013.

Quantum Adiabatic Optimization

Stephen Jordan

Michael Jarret (University of Maryland)

In quantum systems, the allowed energies are often quantized into a discrete set of values. For many applications, the energy gap between the lowest allowed energy and the second-lowest energy is the key property. In particular, a class of quantum algorithms called adiabatic algorithms has been proposed for optimization problems. The runtime of such adiabatic algorithms is determined by this energy gap.

Despite much effort, the energy gaps characterizing proposed adiabatic algorithms have proven very difficult to analyze theoretically. One of the intuitions behind adiabatic algorithms is the idea that adiabatic algorithms are similar to simulated annealing, except that quantum systems can escape from local energy minima via tunneling instead of by thermal excitation. Implicit behind this reasoning is arguably the idea that quantum adiabatic algorithms have no difficulty finding the global energy minimum if there are no other local minima to get trapped in. One result from this project has been the discovery of a counterexample to this intuition. Specifically, we discovered a fairly simple optimization problem on a graph with no local energy minima, which nevertheless has an exponentially small eigenvalue gap.

On the positive side, we have proven that in certain highly regular graphs, such as the path and hypercube graphs, this intuition is correct. That is, the energy gap cannot be small unless there are local energy minima. In fact, our lower bounds for the eigenvalue gaps associated with convex energy landscapes on path graphs is precisely tight and constitutes a discrete analogue to the recently proven fundamental gap theorem regarding Schrödinger operators on \mathbf{R} .

Foundations of Measurement Science for Information Systems

Modern information systems are astounding in their complexity. Software applications are built from thousands of interacting components. Computer networks interconnect millions of independently operating nodes. Large-scale networked applications provide the basis for services of national scope, such as financial transactions and power distribution. In spite of our increasing reliance on such systems, our ability to build far outpaces our ability to secure. Protocols controlling the behavior of individual nodes lead to unexpected macroscopic behavior. Local power anomalies propagate in unexpected ways leading to large-scale outages. Computer system vulnerabilities are exploited in viral attacks resulting in widespread loss of data and system availability. The stability of our critical infrastructure is simply unknown. Measurement science has long provided a basis for the understanding and control of physical systems. Such deep understanding and insight is lacking for complex information systems. We seek to develop the mathematical foundations needed for a true measurement science for complex networked information systems.

Systemic Risks/Benefits of Interconnectivity

Vladimir Marbukh

Assane Gueye

Iraj Saniee (Alcatel Lucent Bell Laboratories)

O. Narayan (University of California at Santa Cruz)

Technological advances combined with economic advantages drive systems towards interconnectivity. This trend has already produced highly interconnected world-wide infrastructures, which are essential for U.S. industrial competitiveness and economic security. However, recent systemic failures of communication, power, financial and other large-scale infrastructures have demonstrated that the economic and social benefits of large scale and interconnectivity come with inherent systemic risks of cascading failures, as well as undesired and malicious behavior. This project concentrates on developing systemic risk metrics that can be used for prediction and mitigation of undesirable system behavior of this type.

In the last several years numerous research centers, think tanks, and working groups have been chartered to address various aspects of systemic risk. The motivation for ACMD's decision to contribute to these interdisciplinary efforts, which encompass areas of complex systems, physics, economics, biology, computational sciences, etc., is twofold. First, ACMD is well positioned due to synergy among existing ITL and NIST programs on complex systems, cyber security, cloud computing, communication networks, smart grid, big data, etc. Second, and more importantly, ITL and NIST must develop competency in these areas due to clear national needs to understand and mitigate systemic risks in critical infrastructures. Our current efforts lie in the following three overlapping areas.

The first area is understanding, prediction and mitigation of cascading overload in the large-scale infrastructures of shared resources. Dynamic resource sharing has both positive and negative effects on sys-

tem performance, with the positive effect resulting from the statistical multiplexing gain, and the negative effect resulting from unavoidable overhead, e.g., due to coordination or delays in accessing distant resources. Motivated by large-scale cloud computing infrastructures, [1] makes a case for the Perron-Frobenius eigenvalue of the mean-field equations linearized about the "operational" system equilibrium to be viewed as a measure of the systemic risk of cascading overload in complex loss resource sharing systems. Draft [2] extends [1] to more realistic service models allowing queuing of requests. In the future we plan to investigate practical applicability and the possibility of real-time estimation of this risk measure.

The second area is quantification and mitigation of networked system performance deterioration due to attack by an intelligent adversary or adversaries. Paper [3] proposes and discusses a game-theoretic framework for (a) evaluating security vulnerability, (b) quantifying the corresponding Pareto optimal vulnerability/cost tradeoff, and (c) identifying the optimal operating point on this Pareto optimal frontier. The vulnerability metric is determined by the Nash equilibrium payoff of the corresponding game. Paper [4] analyses the economics of network vulnerability reduction by considering the tradeoff between system redundancy and component hardening. Our analysis suggests that due to the effect of diminishing return, the optimal vulnerability reduction strategy depends on the specific system cost/preference structure.

Finally, the third area is effect of system information availability on the system performance under normal and adversarial conditions. Routing is the most basic function of a networked system. In the extreme case when global system information is locally available, the routing performance is optimized by "minimum cost routing" with the appropriately defined cost function. In another extreme case when no global information is locally available, i.e., due to high network volatility, random walk routing is the only choice. Paper [5] derives an analytical expression for

the mean load at each node of an arbitrary undirected graph for the uniform multicommodity flow problem under random walk routing. Our analysis shows that the mean load is proportional to the nodal degree with a common multiplier equal to the sum of the inverses of the non-zero eigenvalue of the graph Laplacian. Using this explicit expression for the mean load, [5] gives asymptotic estimates for the load on a variety of graphs with known spectral densities. For graphs with unknown spectral densities [5] gives numerical estimates for the mean load.

- [1] V. Marbukh, Perron-Frobenius Measure of Systemic Risk of Cascading Overload in Complex Clouds: Work in Progress, in *Proceedings of the 6th IFIP/IEEE International Workshop on Distributed Autonomous Network Management Systems*, Ghent, Belgium, May 2013.
- [2] V. Marbukh, Economic Efficiency vs. Systemic Risks in the Cloud Computing Model: Towards Quantitative assessment, in preparation.
- [3] A. Gueye and V. Marbukh, A Game-theoretic Framework for Network Security Vulnerability Assessment and Mitigation, *Lecture Notes in Computer Science* **7638** (2012), *Decision and Game Theory for Security*, 186-200.
- [4] A. Gueye and V. Marbukh, A Cost/Benefit Analysis of Network Vulnerability Reduction: Element Hardening vs. Adding Redundancy, in *Proceedings of W-PIN+NetEcon 2013: The Joint Workshop on Pricing and Incentives in Networks and Systems*, Pittsburgh, PA, June 21, 2013.
- [5] O. Narayan, I. Saniee and V. Marbukh, Congestion Due to Random Walk Routing, arXiv:1309.006.

Examining the Gromov Curvature of Networks in Time

Brian Cloteaux
Vladimir Marbukh

As various networks evolve in time, it has been observed that various characteristics (such as density and diameter) change in some unexpected ways [2]. For instance, if we were to randomly add nodes to some network model, we would expect to see the diameter of the network increase in time. Instead, for various complex networks, we see that the diameter does not grow in time, and many times it actually shrinks. Explanations for this phenomenon are necessary to be able to model and measure these networks.

In looking for an explanation for these observations, we are interested in how the Gromov hyperbolicity of a network changes as the network evolves. Intuitively, Gromov hyperbolicity is a measurement of how close a network is to resembling a

tree. We are interested in seeing whether hyperbolicity changes can account for the network observations.

A difficulty with this type of experiment is that naive computation of Gromov hyperbolicity requires $O(n^4)$ steps. This makes it too expensive to compute for large networks, and is the reason that this simple type of experiment has not been tried before. We are currently using and extending the algorithms produced by INRIA [1] for this type of measurement. We are also working on new approaches to computing this value including fast approximations.

- [1] N. Cohen, D. Coudert, and A. Lancin, Exact and Approximate Algorithms for Computing the Hyperbolicity of Large-scale Graphs, INRIA Research Report RR-8074, September 2012.
- [2] J. Leskovec, J. Kleinberg and C. Faloutsos, Graphs over Time: Densification Laws, Shrinking Diameters and Possible Explanations, in *Proceedings of the 11th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2005.

An Improved Feedback Vertex Set Heuristic

James M. Shook
Isabel Beichl

To recover from deadlock it is sometimes necessary to end processes so that availability of resources can be restored. The trick is to accomplish this by ending the fewest possible processes. To help with these decisions, the relationships between processes can be represented by a directed graph called a dependency graph. If the dependency graph has a cycle, then deadlock has occurred and we need to end a process on that cycle. A feedback vertex set (FVS) is a set of vertices or processes that hits every cycle in the dependence graph. Finding the smallest FVS was shown to be NP-hard in [2]. Thus, research has focused on finding an efficient heuristic for the FVS problem.

In [3], the authors presented a method that finds an FVS, F , with a running time of $O(|F| n^{2.376})$, where n is the number of vertices in the graph. Evidence was given that their algorithm is superior to other existing heuristics. Using an observation made in [1], and relating it to disjoint cycle unions, we designed a method that has a running time of about $O(|F| \log(n) n^2)$. We found that our method is not only faster than previous heuristics, but the size of our FVS is significantly improved over other methods. We give a detailed analysis of our method in a soon to be finished paper.

- [1] I. Beichl and F. Sullivan, Approximating the Permanent via Importance Sampling with Application to the Dimer Covering Problem, *Journal of Computational Physics* **149:1** (1999), 128-147.

- [2] R. Karp, Reducibility among Combinatorial Problems, in *Complexity of Computer Computations* (R. Miller and J. Thatcher, eds.), Plenum Press, 1972, 85-103.
- [3] M. Lemaic and E. Speckenmeyer, Markov-chain-based Heuristics for the Minimum feed-back Vertex Set Problem, Technical Report, 2009.

Broadcast and Spread of Information in Complex Networks

Fern Y. Hunt

We are studying the optimal spread of information in networks where communication and coordination are autonomous and distributed. In a model of such communication, nodes receive information (function values) from their neighbors and broadcast back a weighted average of these values. The issues arising from this research are particularly relevant to control of large networks of nodes with limited communication resources. Examples include sensor networks for energy and water supply, propagation of influence in social networks, and the study of gene regulatory networks.

Following the work of Borkar et al. [1], information spread is studied in terms of a dual process, a random walk on an (assumed strongly connected) graph of the network. A random walk is initiated at a node, i.e., a vertex outside a pre-determined set of *target* nodes, and is halted upon first arrival to that set. The effectiveness of the set is then measured by the sum of the expected times random walkers first arrive starting from outside the set. We can find the most effective target set by minimizing the sum of the expected arrival times over all sets with the same or smaller cardinality. The optimal target set is also optimal for the dual process of spreading. So, if information must be communicated to a large network but resources limit the number of nodes that can be directly contacted, then the quickest way to communicate is to inform the nodes of the optimal target set. The work of Clark et al. [2] also shows that the target nodes are analogous to leader nodes in a leader-follower consensus model. We can demonstrate that a set of effective leaders is also a set of effective target nodes in the random walk model.

The objective function in all these minimizations is a supermodular set function. Most existing results on the computation and approximation of optimal sets are based on the application of the greedy algorithm, a long standing technique for optimizing submodular (supermodular) functions [1, 2]. Unfortunately it is not hard to find examples of graphs where the set constructed by the greedy algorithm fails to be optimal. However the supermodularity of the objective function is used in [1] and [2] to guarantee that the constructed

set is in some sense within $(1-1/e)$ of the optimal, and theoretical work suggests that this is the best possible result. Interestingly, Krause et al. [6] report that “online computations (problem instance dependent)” can reach within 95% of the optimal solution in a sensor placement problem.

Led by our own computations, we reformulated the problem so that optimal or near optimal sets can be constructed. Here, near optimality of a set is defined in terms of its objective function value, which must be bounded above by a constant. Rather than starting with just the graph and the desired cardinality of an unknown set, our method is based on generating vertex covers for the graph. A vertex cover is a set of vertices with the property that every edge of the graph is incident to a vertex in the cover. These sets are optimal spreaders for their cardinality and can be efficiently generated by the greedy algorithm for a maximal match. Since vertex covers frequently contain optimal sets as subsets, one idea is to restrict the search to these sets. Not every maximal match has optimal subsets, however.

Our principal contribution this year is the construction of a subset of optimal and near optimal sets that are the feasible sets for a greedoid. This method may be extendable to general isotone supermodular functions. The properties of this structure imply that near optimal (and possibly optimal) sets can be constructed in a stepwise fashion. The degree of optimality can be specified in advance and all feasible vertex covers of sufficient size (which depends on the degree of optimality) contain near optimal (and possibly optimal) sets. Greedoid properties also permit the construction of a greedoid graph whose nodes are optimal, and near optimal, feasible sets, so it may be possible to improve approximations by local searches in the vicinity of an initial estimate.

The framework sketched here allows the problem

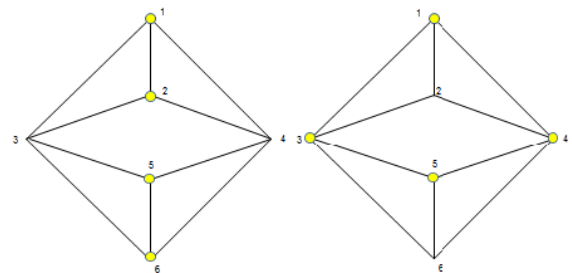


Figure 44. The figure shows a graph with 6 vertices and two distinct (non-automorphic) vertex covers. Vertices of the respective covers are colored. On the right, the vertex cover solves the optimal target (or spread) problem for $K=4$. It contains sets that solve the optimal target problem for $K=1$ ($\{3\}$ or $\{4\}$), $K=2$, ($\{3,4\}$), and $K=3$ ($\{1,3,4\}$). The vertex cover on the left is a solution of the optimization problem for $K=4$, but it contains no optimal sets as proper subsets. Our research seeks to identify vertex covers like those on the right with a view towards searching for optimal subsets of a desired cardinality.

of optimal spread to be considered in the context of the topology of the graph of optimal and near optimal sets. How can they be efficiently computed? Understanding the relationship between the topology of the network graph and the greedoid graph is an important next step to answering this question and is a topic of future research.

- [1] V. Borkar, J. Nair and N. Sanketh, Manufacturing Consensus, in *Proceedings of the 48th Annual Allerton Conference*, 2010, 1550-1555.
- [2] A. Clark, L. Bushnell and R. Poovendran, Leader Selection for Minimizing Convergence Error in Leader-Follower Systems: A Supermodular Optimization Approach, in *Proceedings of the 10th International Symposium on Modeling and Optimization in Mobile Ad Hoc and Wireless Networks (WiOpt)*, 2012, 111-115.
- [3] F. Hunt, Optimal Spread in Network Consensus Models, in review.
- [4] F. Hunt, The Structure of Optimal and Nearly Optimal Target Sets in a Random Walk Model of Spread in a Network, in preparation.
- [5] B. Korte, L. Lovasz and R. Schrader, *Greedoids*, Springer Verlag, 1991.
- [6] A. Krause, J. Leskovec, C. Guestrin, J. Van Briessen and C. Faloutsos, Efficient Sensor Placement Optimization for Securing Large Water Distribution Networks, *Journal of Water Resources Planning and Management* **134** (2008), 516-526.

An Algebraic Formulation for the Analysis and Visualization of Network Graphs

Roldan Pozo

Understanding the topological structure of large graphs remains an important problem in network science. While it is straightforward to visualize small networks of hundreds or a few thousands of vertices and edges using conventional graph visualization packages, attempting to render large real networks is nearly impossible. This is particularly true for information networks and social networks, where the graph sizes number into the millions and billions. And with the amount of data being generated and gathered from large social media sites ever increasing, the challenge of characterizing larger and larger networks is only getting greater.

Conventional algorithms for graph visualization typically render such networks as a solid blot of color in which is difficult to see meaningful information. This difficulty is strongly influenced by the presence of high-degree nodes (hubs) that entangle many parts of the graph with itself, together with the sheer volume of

nodes and edges that makes rendering into a reasonable image size for viewing and printing impractical.

An alternate approach is to visualize important network properties, rather than the actual network itself. For example, such *network portraits* might attempt to capture interesting attributes of a large graph, such as degree distribution, or its connective properties. In our work, we focus on a particular type of information: the distribution of “fringe” communities: small connected components of a graph, in the absence of high-degree hubs. In a social science context, for example, they represent independent or rogue groups, which are highly connected amongst themselves, but which are often lost with the inclusion of more popular nodes.

Consider, for example, a web graph, where nodes are individual web pages, and edges are directed hyperlinks between two web pages. Figure 45, for example, illustrates connected components of the math.nist.gov web graph, where nodes of degree greater than 25 have been removed. The image reveals various structures, such as ladders, stars, and cluster patterns representing tightly coupled web pages. These form the nucleus of fringe communities of web pages, and by varying the degree parameter we can select the size and granularity of groups revealed. As the degree threshold is increased from 1 to the largest degree in the original graph, we can form a connected component size distribution, which can be encoded as a row of a matrix. This sparse matrix may still be too large to view directly, but can be compactly rendered by projecting its nonzero values onto the z-axis and displaying it as a three-dimensional structure, as shown in Figure 46.

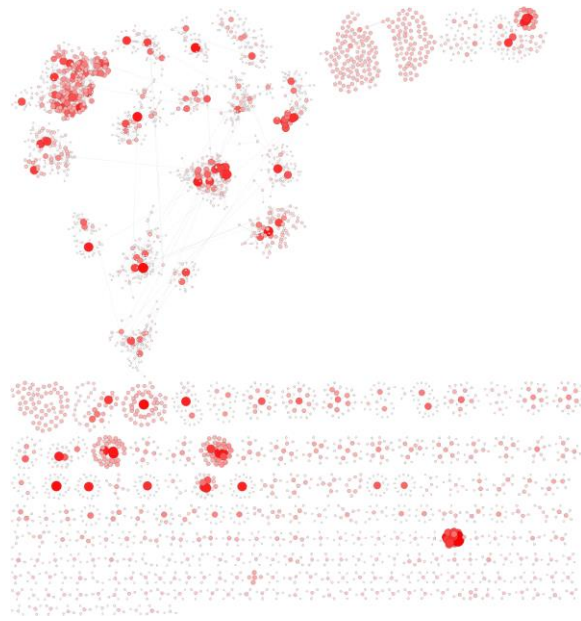


Figure 45. Non-trivial components of math.nist.gov web graph, restricted to nodes with combined degree less than or equal to 25.

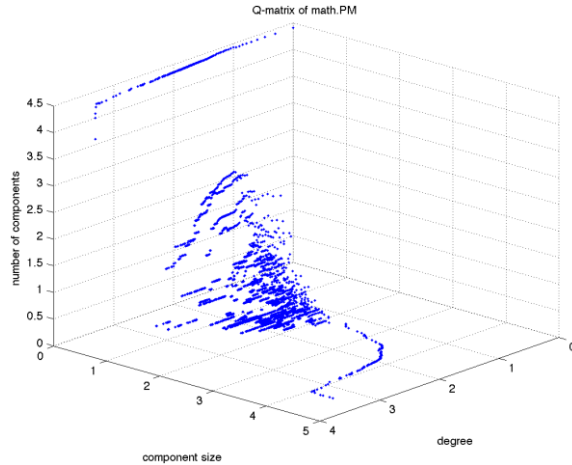


Figure 46. *Q*-matrix plot of math.nist.gov webgraph (29K vertices, 62K edges) showing the component size distribution of degree-limited subgraphs.

The *Q*-matrix of a network, in its fundamental formulation, is a connected component size distribution matrix for a series of degree-limited subgraphs of the original network (or weakly-connected component for directed networks.) Thus, $Q(i,j)$ is the number of connected components of size j in a subgraph where the maximum degree is equal to or less than i .

The *Q*-matrix of a graph can be considered as a generalization of its degree-distribution. However, it encodes other properties, such as the formation and growth of its giant component, its connected subparts, as well as its size parameters. In fact, common network metrics (e.g., degree distribution, number of connected components, number of vertices and edges) can be extracted from the *Q*-matrix using simple linear algebra operations.

Among the interesting characteristics of the *Q*-matrix formulation is that network graphs from similar application areas (e.g., social networks, email networks, web graphs, peer-to-peer networks, road networks, citation graphs) share similar visual characteristics, creating a potential framework for network identification and classification. Indeed, we have used the *Q*-matrix formulation to generate meaningful thumbnail images for network data collections. Finally, the computation of the *Q*-matrix is highly efficient. Graphs with millions of vertices and edges can be processed in seconds on common desktop computers.

We are extending research of *Q*-matrix theory to generalized vertex orderings beyond that of node degree, such as PageRank, eigenvalue centrality, betweenness centrality, and k -core numbers. Furthermore, we are investigating the use of *Q*-matrix analysis to specific problems in the area of microbiology (genomic networks) and economics (financial market networks).

[1] R. Pozo, Efficient *Q*-matrix Computation for the Visualization of Complex Networks, in *Proceedings of*

Complex Networks Workshop, Eighth International Conference on Signal Image Technology and Internet Based Systems, Sorrento, Italy, Nov. 25-29, 2012, 762-767.

Security Risk Analysis of Enterprise Networks using Attack Graphs

Anoop Singhal (NIST ITL)

S. Jajodia (George Mason University)

Lingyu Wang (Concordia University)

At present, computer networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems, and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and security of the nation. Vulnerabilities are regularly discovered in software applications that are exploited to stage cyber-attacks. Currently, management of security risk of an enterprise network is more an art than a science. System administrators operate by instinct and experience rather than relying on objective metrics to guide and justify decision making.

The objective of this research is to develop a standard model for security risk analysis of computer networks. A standard model will enable us to answer questions such as “Are we more secure now than yesterday?” or “How does the security of one network configuration compare with another one?” Also, having a standard model to measure network security will allow users, vendors, and researchers to evaluate methodologies and products for network security in a coherent and consistent manner.

In this project, we have approached the challenge of network security analysis by capturing vulnerability interdependencies and measuring security in the exact way that real attackers penetrate the network. Our methodology for security risk analysis is based on the model of attack graphs. We analyze all attack paths through a network, providing a probabilistic metric of the overall system risk. Using this metric, we analyze trade-offs between security costs and security benefits.

Computer systems are vulnerable to both known and previously unknown (zero day) attacks. Handling zero day vulnerabilities is inherently difficult due to their unpredictable nature. In FY 2013, we attempted to assess the risk of unknown attack patterns. We developed a new model “ k -zero day safety” for zero day attacks. Existing algorithms for computing this metric are not scalable as they assume that a complete zero day attack graph has been generated. We have proposed a set of polynomial time algorithms for estimating k -zero day safety. Our paper on this topic [1] received the Best Paper award at the 10th International Conference on Security and Cryptography.

Measuring the mean time to compromise of a network provides important insights for understanding a network's vulnerability to attacks. We have proposed a unified framework for measuring a network's mean time to compromise by considering both known and zero day attacks. This approach was published in a paper in the IEEE Symposium on Reliable and Distributed Systems [2]. We have also shown an application of this framework to network hardening.

In FY 2014, we plan to apply attack graphs to study the effect of diversity for network defense. We also plan to publish the results as a NIST report and as white papers in conferences and journals.

- [1] M. Albanese, S. Jajodia, A. Singhal, and L. Wang, An Efficient Approach to Assessing the Risk of Zero-day Vulnerabilities, in *Proceedings of the 10th International Conference on Security and Cryptography (SECRYPT 2013)*, Reykjavik, Iceland, July 29-31, 2013.
- [2] W. Nzoukou, L. Wang, S. Jajodia and A. Singhal, A Unified Framework for Measuring a Network's Mean Time-to-compromise, in *Proceedings of the 32nd IEEE International Symposium on Reliable Distributed Systems (SRDS 2013)*, Braga, Portugal, September 30 - October 3, 2013.

[This research was sponsored in part by ACMD.]

Combinatorial Testing

Raghu Kacker

D. Richard Kuhn (NIST ITL)

Yu Lei (University of Texas at Arlington)

James Lawrence (George Mason University)

Combinatorial testing (CT) is an approach to detect combinatorial interaction faults, which may cause a software based system to fail when certain values of some factors occur together. Combinatorial testing is based on the insight, referred to as the *interaction rule*, that while the behavior of a software system may be affected by a large number of factors, only a few factors are involved in a failure-inducing fault. Many critical system failures in recent times have been traced to interaction faults in the underlying software. Studies of actual faults reveal that most involve only one or two factors, though some may involve up to six.

NIST has taken the lead to advance software testing technology from pair-wise to higher strength testing, to make tools and techniques available to US industry, and to help promote its effective use. As a result of these efforts, CT is being increasingly used in a wide spectrum of industries and taught in colleges. CT is a versatile and broadly applicable methodology that is helping to reduce testing costs and efforts in software based systems for science, commerce, defense and security, and electronic medical systems, and is

increasingly used in hardware testing as well. A recent paper from the US Lockheed Martin Company reports 20% savings in test efforts.

ACTS is a NIST/UTA (University of Texas at Arlington) tool to generate high strength test suites for CT. A key feature of ACTS is support of constraints among factor and test values. We have filled more than 1600 requests for ACTS, and the tutorial has been downloaded more than 26000 times.

CCM is a new NIST tool to determine combinatorial coverage of a test suite that was not developed from a CT viewpoint. The latest version of CCM supports constraints and has a greatly improved graphical depiction of combinatorial coverage. A parallel processing version of CCM is also available. Combinatorial deficiency of a test suite can be remedied by including additional tests, so CCM can help a test suite satisfy combinatorial requirements.

A book on CT entitled, *Introduction to Combinatorial Testing*, by D. R. Kuhn, R. N. Kacker and Y. Lei was published by the CRC Press in 2013.

This year we demonstrated the effectiveness of CT for conformance testing and interoperability testing of portable healthcare devices. The ISO/IEEE 11073 is a set of standards for interoperability of personal healthcare devices. We developed a framework and a research tool for conformance and interoperability testing to the IEEE 11073 standards. Testing using these methods detected two faults, one of which was a new discovery.

We organized the second International Workshop on Combinatorial Testing (IWCT) in conjunction with 6th IEEE International conference of software testing (ICST) in Luxembourg to bring together researchers, developers, users, and practitioners to exchange ideas and experiences with CT methods and tools. Seventeen excellent papers were selected by the Program Committee and were presented in talk or poster format. The

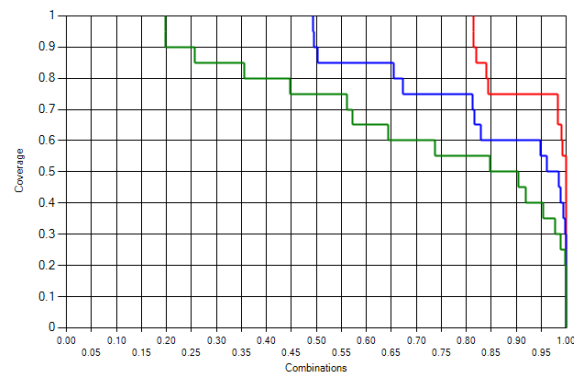


Figure 47. Combinatorial coverage for a test suite of 79 factors (seventy five with 2 test settings, two with 4 test setting and two with six test settings); horizontal-axis indicates fractions of the 2-way, the 3-way, and the 4-way combinations and vertical-axis shows corresponding percent covered with 7489 tests in a project of Johns Hopkins University Applied Physics Laboratory.

third IWCT is scheduled for March 31, 2014 in Cleveland, Ohio. We also organized the First Asian Workshop on Combinatorial Testing for Complex Computer Systems (AWCTCCS) in conjunction with 18th IEEE International Conference on Engineering of Complex Computer Systems (ICECCS) on July 19, 2013 at the National University of Singapore. It consisted of six presentations and one discussion session. A joint presentation with NASA employees demonstrating effectiveness of CT was made at NASA's Annual Workshop on Independent Verification and Validation of Software, Sept. 10-12, 2013.

A team of four students from the Carnegie Mellon University is working with NIST on a master's degree project to develop a tool that enhances the ability of testers to define an input model, and streamline the testing process. This will make CT easier to use and should improve results, since testers will have a better understanding of system characteristics.

Working with the NIST Computer Security Division and representatives and contractors of the General Services Administration, the team is developing a set of test specifications for the Personal Identity Verification (PIV) cards used throughout government. The objectives are to improve interoperability testing with fewer tests, and to develop procedures for computing the number of tests required for various PIV card specifications.

Our research and tool development continues on input space modeling for CT, integration of test generation tools in large testing infrastructure and on automating determination of expected output for each test case. We continue to explore opportunities of application of CT in defense and security, electronic healthcare IT systems, and cloud computing systems.

- [1] D. R. Kuhn, R. N. Kacker and Y. Lei, *Introduction to Combinatorial Testing*, CRC Press, 2013.
- [2] R. N. Kacker, D. R. Kuhn, Y. Lei and J. F. Lawrence, Combinatorial Testing for Software: an Adaptation of Design of Experiments, *Measurement* **46** (2013), 3745-3752.
- [3] L. Yu, Y. Lei, R. Kacker and D. R. Kuhn, R. Sriram and K. Brady, A General Conformance Testing Framework for IEEE 11073 PHD's Communication Model, in *Proceedings of 6th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA)*, Greece, May 29-31, 2013.
- [4] L. Yu, Y. Lei, R. Kacker and D. R. Kuhn, ACTS: A Combinatorial Test Generation Tool, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST-2013)*, Luxembourg, March 18-22, 2013.
- [5] L. Yu, M. N. Borazjany, Y. Lei, R. N. Kacker and D. R. Kuhn, An Efficient Algorithm for Constraint Handling in Combinatorial Test Generation, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST-2013)*, Luxembourg, March 18-22, 2013.
- [6] M. N. Borazjany, L. S. G. Ghandehari, Y. Lei, R. Kacker and D. R. Kuhn, An Input Space Modeling Methodology for Combinatorial Testing, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST-2013)*, Luxembourg, March 18-22, 2013.
- [7] L. S. G. Ghandehari, M. N. Borazjany, Y. Lei, R. Kacker and D. R. Kuhn, Applying Combinatorial Testing to the Siemens Suite, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST-2013)*, Luxembourg, March 18-22, 2013.
- [8] D. R. Kuhn, I. Dominguez Mendoza, R. N. Kacker and Y. Lei, Combinatorial Coverage Measurement Concepts and Applications, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST-2013)*, Luxembourg, March 18-22, 2013.
- [9] R. Kacker, D. R. Kuhn, Y. Lei and J. Lawrence, Combinatorial Testing for Software used in Metrology, in *Proceedings of XX IMEKO World Congress*, Busan, Republic of Korea, September 9-14, 2012.

Coverage and Energy Optimization in Mobile Sensor Networks

Vladimir Marbukh

Kamran Sayrafian

Amir Aghdam (Concordia University)

Hamid Mahboubi (Concordia University)

Kaveh Moezzi (Concordia, University)

Mobile sensor networks (MSNs) are envisioned to enable a novel set of applications in detecting, monitoring and tracking people, targets or events in pervasive computing environments. Locations of sensors in a MSN affect both their ability to acquire information on the intended target(s) and event(s) as well as their ability to communicate this information to the intended recipient(s). The information acquisition needs, which require proximity to the target(s), often compete with the communication needs, which require proximity to the recipient(s) of the sensor information. Inherent traits of MSN such as lack of centralized control, variety of performance criteria, operational uncertainties, possibilities of MSN topology change and sensor trapping in suboptimal locations make MSN optimization an exceedingly challenging problem.

Our previous publications proposed aligning sensor mobility with the overall MSN goals by assuming that (a) sensing and communication are optimized much faster than sensors relocate, and (b) sensor relocations are governed by cost/benefit analysis where "cost" of sensor battery energy expenditure for sensor relocation is weighed against projected performance gains due to new sensor locations. Practicality of this

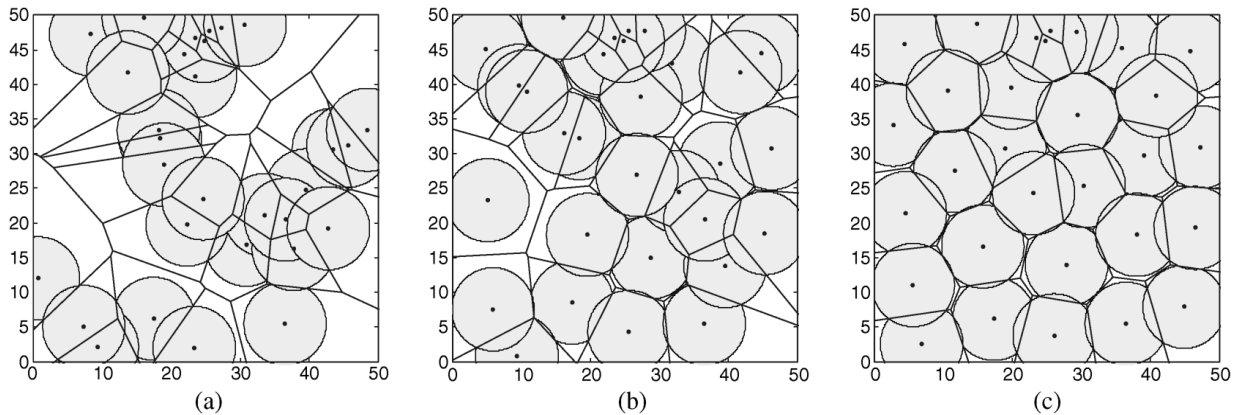


Figure 48. Movement of sensors as well as the Voronoi polygons and sensing circles (a) Initial configuration (b) Configuration after the first round. (c) Final configuration.

framework depends on overcoming numerous challenges with the (inherently) distributed nature of MSN being the most critical. An intelligent sensor may be able to estimate its current life expectancy from its battery energy level and depletion rate affected by the surrounding terrain as well as sensor information acquisition and transmission capabilities. However, a sensor typically has no direct knowledge of the effect of its relocation on the rest of the MSN. Current research attempts to address some of these issues.

We have studied target monitoring using a network of collaborative mobile sensors in [1]. The objective is to compute the desired sensing and communication radii of the sensors as well as their locations at each time instant, such that a set of prescribed specifications is met. These specifications include end-to-end connectivity preservation from the target to a fixed destination, while longevity of sensors is maximized and the overall energy consumption is minimized. The problem is formulated as a constrained optimization problem, and a procedure for solving this problem is presented. Simulation results demonstrate the effectiveness of the proposed techniques.

Efficient sensor deployment strategies developed to increase coverage in wireless mobile sensor networks have been investigated in [2]. The sensors identify coverage holes within their Voronoi polygons, and then relocate to minimize these coverage holes. Novel edge-based and vertex based relocation strategies have been proposed, and their performances are compared with existing strategies. The proposed sensor relocation strategies are based on the distances for each sensor between the points inside the Voronoi polygon and the edges or vertices of the polygon. It is shown that the methods introduced in [2] outperform existing strategies. Simulations confirm the effectiveness of our deployment algorithms and their superiority to the techniques reported in the literature. Figure 48 demonstrates sample evolution of coverage area (along

with the corresponding Voronoi regions) under an edge-based strategy.

Continuing this work, we plan to investigate joint sensor motion and coverage radius optimization as an example of a cyber-physical system that involves co-design of physical and cyber components.

- [1] H. Mahboubi, A. Momeni, A.G. Aghdam, K. Sayrafian and V. Marbukh, An Efficient Target Monitoring Scheme with Controlled Node Mobility for Sensor Networks, *IEEE Transactions on Control Systems Technology* **20:6** (November 2012), 1522-1533.
- [2] H. Mahboubi, K. Moezzi, A. Aghdam, K. Sayrafian, and V. Marbukh, Distributed Deployment Algorithms for Improved Coverage in a Network of Wireless Mobile Sensors, *IEEE Transactions on Industrial Informatics*, accepted.

A Dynamic Computational Phantom for RF Propagation in Body Area Networks

John Hagedorn
Kamran Sayrafian
Martina Barbi
Judith Terrill

A body area network (BAN) is a radio communication and networking protocol for short range, low power and highly reliable wireless connectivity for use inside or around a human body. It includes radio frequency (RF) enabled devices that could be implanted, worn or located adjacent to the body. Radio-enabled implantable sensor nodes offer a revolutionary set of applications, among which are smart pills for precision drug delivery, glucose monitors, blood pressure monitors, and eye pressure sensors for glaucoma patients. At the same time, wearable sensor nodes can enable remote wireless monitoring of electrocardiogram (ECG),



Figure 49. Sequence of poses emulating walking in the human body model.

temperature, respiration, and heart rate. While BAN is poised to be a promising technology with novel uses in pervasive healthcare, there are still many technical, commercial and regulatory challenges, including usability, interoperability, energy source, miniaturization, security, and privacy. A prerequisite for the safe and effective design of such systems is an understanding of RF propagation around and inside the body.

Efficient transceiver design for implants or wearable devices requires in-depth understanding of the propagation media, i.e., the human body. Due to the difficulties of performing experiments with human subjects, obtaining sufficient amounts of measurement data for such use-cases is extremely difficult or in some cases nearly impossible. So we have developed a unique 3D modeling and visualization platform that allows virtual RF propagation experiments to be performed using aposable human body computational phantom [1, 2].

As body motion could significantly impact the wireless communication between implants and wearable medical sensors, a dynamic computational phantom capable of emulating human motion would be a valuable tool to study and understand this impact. Our objective in this project is to create a dynamic computational phantom as an extension to our existing static body model. The dynamic phantom would be capable of emulating human motion such as walking, rolling in a bed, twisting/turning, and bending. To accomplish this, we have developed computational methods for deforming the 3D body model (including the internal body organs) into various poses. We have used these methods to create a sequence of poses to describe motion such as walking. Figure 49 shows four walking poses [2]. The posed body models will be used as the basis for a series of simulations.

We plan to use our system to study the effects of body pose and motion on RF propagation in BAN. This is referred to as dynamic channel and it is a more realistic scenario of operation of wearable and implantable sensors in a human body. Through collaborative efforts with other research institutes, we compare the results of our simulations with experimental results. We anticipate that these efforts will accelerate the commercial

development of BAN technology along with its related standards.

- [1] K. Sayrafian-Pour, J. Hagedorn, W. Yang and J. Terrill, "A Virtual Reality Platform to Study RF Propagation in Body Area Networks," 3rd IEEE International Conference on Cognitive Infocommunications, Kosice, Slovakia, December 5, 2012.
- [2] J. Hagedorn, K. Sayrafian and J. Terrill, "A Dynamic Human Body Computational Phantom for RF Propagation Study," 4th International Workshop on Computational Phantoms, Zurich, Switzerland, May 2013.

Evaluation and Mitigation Strategies for Cross-Interference between Multiple Body Area Networks

Kamran Sayrafian

Martina Barbi

Vladimir Marbukh

John Hagedorn

Judith Terrill

Mehdi Alasti (Time Warner Cable)

Body Area Networks (BANs) consist of multiple wearable (or implantable) sensors that can establish two-way wireless communication with a controller node that could be either worn or located in the vicinity of the body. Considering the mobile nature of BANs along with their proposed operational frequency bands, these networks are expected to coexist with other wireless devices that are operating in their proximity. Therefore, interference from coexisting wireless networks or other nearby BANs could create problems on the reliability of the network operation.

Assuming that a single BAN uses a Time Division Multiple Access protocol to establish communication among its controller and body sensors, there will be no simultaneous transmission, and therefore no interference among nodes of a single BAN. However, when several BANs are within close proximity of each other, interference may occur since no coordination across separate networks exists in general. Hence, the increasing number of such BANs in short proximity of each other could result in performance degradation of one or several communication links. Even when there is a small number of adjacent body area networks, the received signal strength from nearby interfering BANs may be too high, resulting in overwhelming of the desired signal within a particular BAN, therefore causing performance degradation in detecting or decoding the transmitted data.

The complexity associated to BAN communication channels [1, 5] along with the mobility of the subjects wearing BANs could create various compli-

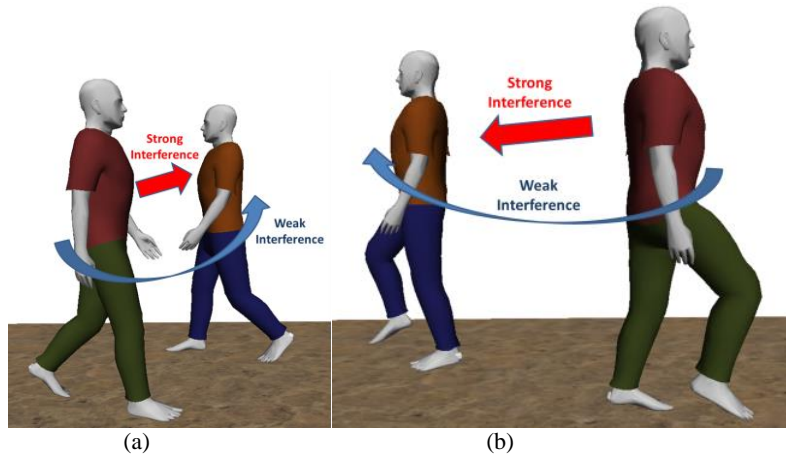


Figure 50. Cross-interference instances among two BANs.

cated scenarios where inter-BAN interference has a negative impact on the reliable reception of data within one BAN. Figure 50 illustrates this point with a simple scenario involving two people who are wearing multiple sensors on the front and back sides of their bodies. When the bodies are face-to-face (i.e., Figure 50a), the line-of-sight channel among the two sensors located on their chests might lead to a strong cross-interference. As they cross each other, the shadowing created by the bodies would remove the interference on the chest sensors; however, line-of-sight among the back sensors (Figure 50b) could lead to interference at that location.

We have developed a simulation platform that allows for statistical evaluation of interference in multi-BAN scenarios [2]. Figure 51 shows a typical scenario where multiple BANs (represented by circles) can be distributed in a virtual room. Each BAN, including a coordinator and several sensor nodes, can move in a given direction. This is meant to represent random walking of people (wearing BANs) inside a room. Initial position and speed of all BANs are programmable.

Statistical knowledge of the amount and characteristics of the inter-BAN interference in various scenarios would be essential information to have in order to study communication link reliability in a body area network. So far, few studies have been done of the impact of such inter-BAN interference. A comprehensive study would eventually require an extensive measurement campaign with networks that have been implemented according to the BAN standard. Until then, a simulation platform that can allow researchers to gain more information about the impact of interference would be an extremely valuable tool. In addition, such a platform could be used to study the performance

of various interference mitigation techniques such as link adaptation and coordinated (or un-coordinated) transmission scheduling algorithms [3]. By distributing simultaneous (i.e., colliding) multi-BAN transmissions across several time slots, inter-BAN interference can be mitigated to some extent [4]. This study is currently underway. We also plan to use this platform to better understand the effectiveness of link layer adaptation in mitigating interference.

- [1] R. Chávez-Santiago, K. Sayrafian, A. Khaleghi, K. Takizawa, J. Wang, I. Balasingham and H.-B. Li, Propagation Models for IEEE 802.15.6 Standardization of Implant Communication in Body Area Networks, *IEEE Communications* **51:8** (2013), 80-87.
- [2] K. Sayrafian, J. Hagedorn, M. Barbi, J. Terrill and M. Alasti, A Simulation Platform to Study Inter-BAN Interference, in *Proceedings of the 4th IEEE International Conference on Cognitive Infocommunications*, Budapest, Hungary, December 2-5, 2013.
- [3] M. Alasti, M. Barbi, K. Sayrafian and R. Verdone, Inter-BAN Interference Evaluation & Mitigation: A Preliminary Study, in *Proceedings of COST IC1004 TD(13)08060*, Ghent, Belgium, September 25-27, 2013.
- [4] V. Marbukh, K. Sayrafian and M. Alasti, Link-layer Adaptation in Body Area Networks: Balancing Reliability and Longevity, in *Proceedings of the 24th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (IEEE PIMRC 2013)*, London, UK, September 2-5, 2013.
- [5] K. Sayrafian, J. Hagedorn, W.-B. Yang and J. Terrill, A Virtual Reality Platform to Study RF Propagation in Body Area Networks, in *Proceedings of the 3rd IEEE International Conference on Cognitive Infocommunications*, Kosice, Slovakia, December 2-5, 2012.

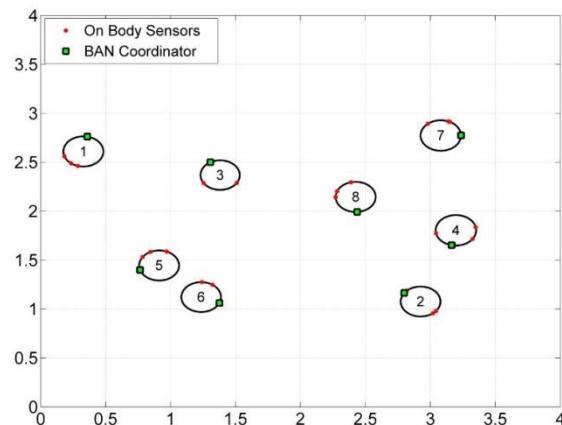
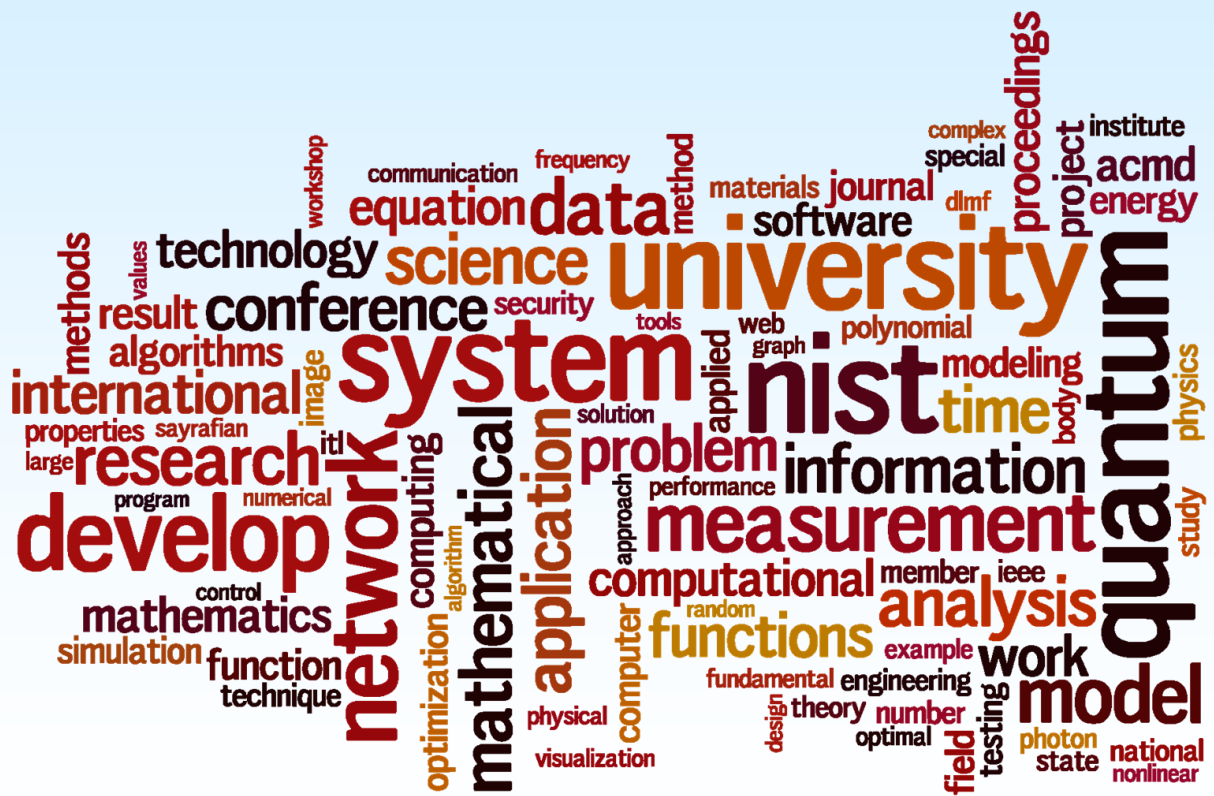


Figure 51. Sample multi-BAN scenario in a 4 m x 4 m rectangular room.

Part IV

Activity Data



Publications

Note: Names of (co-)authors with a Division affiliation during this reporting period are underlined.

Appeared

Refereed Journals

1. B. K. Alpert, R. D. Horansky, D. A. Bennett, W. B. Doriese, J. W. Fowler, A. Hoover, M. W. Rabin and J. N. Ullom, Operation of Gamma-Ray Microcalorimeters at Elevated Count Rates Using Filters with Constraints, *Review of Scientific Instruments* **84** (2013), 056107.
2. F. Backeljauw, S. Becuwe, A. Cuyt, J. Van Deun and D. Lozier, Validated Evaluation of Special Mathematical Functions, *Science of Computer Programming* **10** (2013), 1016.
3. B. D. Bookatz, S. P. Jordan, Y.-K. Liu and P. Wocjan, Quantum Nonexpander Problem Is Quantum-Merlin-Arthur-Complete, *Physical Review A* **87** (2013), 042317.
4. G. W. Bryant, N. Malkova and J. S. Sims, Mechanism for Controlling the Exciton Fine Structure in Quantum Dots using Electric Fields: Manipulation of Exciton Orientation and Exchange Splitting at the Atomic Scale, *Physical Review B* **88** (2013), 161301(R).
5. M. Campanelli, R. N. Kacker and R. Kessel, Variance Gradients and Uncertainty Budgets for Nonlinear Measurement Functions with Independent Inputs, *Measurement Science and Technology* **24** (2013), 025002.
6. R. Chávez-Santiago, K. Sayrafian, A. Khaleghi, K. Takizawa, J. Wang, I. Balasingham and H.-B. Li, Propagation Models for IEEE 802.15.6 Standardization of Implant Communication in Body Area Networks," *IEEE Communications Magazine* **51:8** (Aug. 2013), 80-87.
7. H. S. Cohl, Erratum: Developments in Determining The Gravitational Potential Using Toroidal Functions, *Astronomische Nachrichten* **333:8** (2012), 784-785.
8. H. S. Cohl and H. Volkmer, Definite Integrals Using Orthogonality and Integral Transforms, *Symmetry, Integrability and Geometry Methods and Applications* **8** (2012), 077.
9. H. S. Cohl, Fourier, Gegenbauer and Jacobi Expansions for a Power-Law Fundamental Solution of the Polyharmonic Equation and Polyspherical Addition Theorems, *Symmetry, Integrability and Geometry Methods and Applications* **9** (2012), 042.
10. H. S. Cohl, Fourier Expansions for a Logarithmic Fundamental Solution of the Polyharmonic Equation, *Journal of Classical Analysis* **2:2** (2013), 107-127.
11. H. S. Cohl and H. Volkmer, Separation of Variables in an Asymmetric Cyclidic Coordinate System, *Journal of Mathematical Physics* **54:6** (2013), 063513.
12. H. S. Cohl, C. MacKenzie and H. Volkmer, Generalizations of Generating Functions for Hypergeometric Orthogonal Polynomials with Definite Integrals, *Journal of Mathematical Analysis and Applications* **407:2** (2013), 211-225.
13. H. S. Cohl and H. Volkmer, Publisher's Note: Separation Of Variables in an Asymmetric Cyclidic Coordinate System, *Journal of Mathematical Physics* **54:7** (2013), 079904.
14. H. S. Cohl, On a Generalization of the Generating Function for Gegenbauer Polynomials, *Integral Transforms and Special Functions* **24:10** (2013), 807-816.
15. H. S. Cohl and C. MacKenzie, Generalizations And Specializations Of Generating Functions for Jacobi, Gegenbauer, Chebyshev and Legendre Polynomials with Definite Integrals, *Journal of Classical Analysis* **3:1** (2013), 17-33.
16. D. G. Harris, I. Beichl and F. Sullivan, Fast Sequential Importance Sampling to Estimate the Graph Reliability Polynomial, *Algorithmica* **68** (2014), 916-939, (published online Nov. 8, 2012).
17. R. L. Jacobsen, R. D. Johnson III, K. K. Irikura and R. N. Kacker, Anharmonic Vibrational Frequency Calculations are not Worthwhile for Small Basis Sets, *Journal of Chemical Theory and Computation* **9** (2013), 951-954.
18. R. N. Kacker, D. R. Kuhn, Y. Lei and J. F. Lawrence, Combinatorial Testing For Software: An Adaptation Of Design Of Experiments, *Measurement* **46** (2013), 3745-3752.
19. R. Kessel, R. N. Kacker and K. D. Sommer, Uncertainty Budgeting For Range Calibration, *Measurement* **45** (2012), 1661-1669.
20. A. J. Kearsley, Constrained Hierarchical Control of a Diffusion Equation, *International Journal of Applied Mathematics and Statistics* **35:5** (2013), 5-19.
21. Y.-S. Kim, O. Slattery, P. S. Kuo and X. Tang, Conditions For Two-Photon Interference with Co-

- herent Pulses, *Physical Review A* **87** (2013), 063843.
22. P. S. Kuo, O. Slattery, Y.-S. Kim, J. S. Pelc, M. M. Fejer and X. Tang, Spectral Response of an Up-conversion Detector and Spectrometer, *Optics Express* **21:19** (2013), 22523.
 23. P. S. Kuo, J. S. Pelc, O. Slattery, Y.-S. Kim, M. M. Fejer and X. Tang, Reducing Noise in Single-photon Frequency Conversion, *Optics Letters* **38:8** (2013), 1310.
 24. L. Ma, O. Slattery and X. Tang, Single Photon Frequency Up-Conversion and its Applications, *Physics Reports*, **521:2** (2012), 69-94.
 25. F. Maggioni, F. A. Potra and M. Bertocchi, Optimal Kinematics of a Looped Filament, *Journal of Optimization Theory and Applications* **159** (2013), 489-506.
 26. H. Mahboubi, W. Momeni, A. Aghdam, K. Sayrafian-Pour and V. Marbukh, An Efficient Target Monitoring Scheme with Controlled Node Mobility For Sensor Networks, *IEEE Transactions on Control* **20:6** (2012), 1522-1532.
 27. L. A. Melara and A. J. Kearsley, The Radius of Attraction for Newton's Method and TV-Minimization Image Denoising, *Applied Mathematics Letters* **25:12** (2012), 2417-2422.
 28. W. Mitchell, A Collection of 2D Elliptic Problems for Testing Adaptive Grid Refinement Algorithms, *Applied Mathematics and Computation* **220** (2013), 350-364.
 29. A. Nurse, G. McFadden and S. Coriell, Bubble Motion and Size Variation during Thermal Migration with Phase Change, *Physics of Fluids* **25** (2013), 013302.
 30. D. P. O'Leary and B. W. Rust, Variable Projection for Nonlinear Least Squares Problems, *Computational Optimization and Applications* **54** (2013), 579-593.
 31. K. Pahlavan, G. Bao, Y. Ye, S. Makarov, U. Khan, P. Swar, D. Cave, A. Karellas, P. Krishnamurthy and K. Sayrafian, RF Localization for Wireless Video Capsule Endoscopy, *International Journal of Wireless Information Networks* **19:4** (December 2012), 326-340.
 32. R. Sekerka, W. Boettinger and G. McFadden, Surface Morphologies due to Grooves at Moving Grain Boundaries having Stress-Driven Fluxes, *Acta Materialia* **61** (2013), 7216-7226.
 33. O. Slattery, L. Ma, P. Kuo, Y.-S. Kim and X. Tang, Frequency Correlated Bi-Photon Spectroscopy using a Tunable Up-Conversion Detector, *Laser Physics Letters* **10** (2013), 075201.
 34. Y. Zhang, S. Glancy and E. Knill, Efficient Quantification of Experimental Evidence Against Local Realism, *Physical Review A* **88** (2013), 052119.

Journal of Research of NIST

1. A. S. Carasso and A. E. Vldar, Fractional Diffusion, Low Exponent Levy Stable Laws and 'Slow Motion' Denoising of Helium Ion Microscope Imagery, *Journal of Research of the NIST* **117** (2012), 199-142.
2. A. S. Carasso, Hazardous Continuation Backward in Time in Nonlinear Parabolic Equations, and an Experiment in Deblurring Nonlinearly Blurred Imagery, *Journal of Research of the NIST* **118** (2013), 199-217.

Books

1. D. R. Kuhn, R. N. Kacker and Y. Lei, *Introduction to Combinatorial Testing*, Chapman & Hall/CRC Innovations in Software Engineering and Software Development Series, Taylor & Francis Group, Boca Raton Florida, 2013.

Conference Proceedings

1. M. Alasti, M. Barbi, K. Sayrafian and R. Verdone, Inter-BAN Interference Evaluation & Mitigation: A Preliminary Study, in *Proceedings of the Cooperative Radio Communications for Green Smart Environments Meeting* (IC1004) TD (13)08060, Ghent, Belgium, Sept. 25-27, 2013.
2. M. N. Borazjany, L. S. G. Ghandehari, Y. Lei, R. N. Kacker and D. R. Kuhn, An Input Space Modeling Methodology for Combinatorial Testing, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Luxembourg, March 2013, Second International Workshop on Combinatorial Testing (IWCT-2013), paper 2.
3. B. Cloteaux, Limits in Modeling Power Grid Topology, in *Proceedings of the IEEE Network Science Workshop*, West Point, NY, April 2013, 16-22.
4. J. Conroy, S. T. Davis, J. Kubina, Y.-K. Liu, D. P. O'Leary and J. D. Schlesinger, Multilingual Summarization: Dimensionality Reduction and a Step towards Optimal Term Coverage, in *Proceedings of the Workshop on Multilingual Multi-document Summarization (MultiLing 2013)*, Sofia, Bulgaria, August 2013, 55-63.

5. C. F. Ferraris, N. Martys and W. L. George, Development of Standard Reference Materials for Cement-Based Materials, in *Proceedings of SCC2013, Fifth North American Conference on the Design and Use of Self-Consolidating Concrete*, Chicago, IL, May 12-15, 2013.
6. C. Flynt, P. Brooks and D. G. Porter, Characterizing and Back-Porting Performance Improvement, in *Proceedings of the 20th Annual Tcl/Tk Conference*, New Orleans, LA, September 2013, 53-64.
7. J. T. Fong, J. J. Filliben and A. N. Heckert, A Stochastic and Local Theory of Fatigue for Aging Pressure Vessels and Piping, in *From Failure to Better Design, Manufacture and Construction, Proceedings of 2012 International Symposium on Structural Integrity (ISSI2012)*, S. T. Tu, Z. D. Wang, and G. C. Sih, Eds., Jinan, China, October 31 – Nov. 2, 2012, 19-31.
8. J. T. Fong, W. F. Guthrie, J. J. Filliben and A. N. Heckert, A Bayesian Quantitative Nondestructive Evaluation (Q-NDE) Approach to Estimating Remaining Life of Aging Pressure Vessels and Piping, in *Proceedings of the 2012 Quantitative Nondestructive Evaluation Conference*, Denver, CO, July 2012.
9. J. T. Fong, C. Cimini, D. Melo, J. J. Filliben and A. N. Heckert, Theoretical Failure Envelopes of Open Hole Composite Laminates with A- and B-bases Allowables Estimated from Smooth Specimen Properties, in *Proceedings of 2013 International Conference on Composites Design*, Montreal, Canada, July 2013.
10. J. T. Fong, W. F. Guthrie, A. N. Heckert and J. J. Filliben, A Bayesian Quantitative NDE Approach to Estimating Remaining Life of Aging Pressure Vessels and Piping, in *Proceedings of 2013 International Conference on Structural Mechanics in Reactor Technology (SMiRT-22)*, San Francisco, CA, August 2013, Paper 991.
11. L. S. G. Ghandehari, M. N. Borazjany, Y. Lei, R. N. Kacker and D. R. Kuhn, Applying Combinatorial Testing to the Siemens Suite, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Luxembourg, March 2013, Second International Workshop on Combinatorial Testing (IWCT-2013), paper 4.
12. A. Gueye and V. Marbukh, A Game-theoretic Framework for Network Security Vulnerability Assessment and Mitigation, *Lecture Notes in Computer Science* **7638** (2012), *Decision and Game Theory for Security*, 186-200.
13. A. Gueye and V. Marbukh, A Cost/Benefit Analysis of Network Vulnerability Reduction: Element Hardening vs. Adding Redundancy, in *Proceedings of the Joint Workshop on Pricing and Incentives in Networks and Systems (W-PIN+NetEcon)*, Pittsburgh, PA, June 21, 2013.
14. J. Hagedorn, K. Sayrafian and J. Terrill, A Dynamic Human Body Computational Phantom for RF Propagation Study, in *Proceedings of the Workshop on Computational Phantoms for Radiation Protection, Imaging, and Radiotherapy*, Zurich, Switzerland, May 20-22, 2013.
15. J. Jankowski, S. Ressler, J. Behr, Y. Jung, K. Sons and P. Slusallek, Declarative Integration of Interactive 3D Graphics into the World-Wide Web: Principles, Current Approaches, a Research Agenda, in *Web3D '13: Proceedings of the 18th International Conference on 3D Web Technology*, San Sebastian, Spain, June 20-22, 2013, 39-45.
16. R. N. Kacker, D. R. Kuhn, Y. Lei and J. F. Lawrence, Combinatorial Testing for Software used in Metrology, in *Proceedings of XX IMEKO World Congress*, Busan, Republic of Korea, September 2012.
17. D. R. Kuhn, I. Dominguez-Mendoza, R. N. Kacker and Y. Lei, Combinatorial Coverage Measurement Concepts and Applications, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Luxembourg, March 2013, Second International Workshop on Combinatorial Testing (IWCT-2013), paper 7.
18. P. S. Kuo, J. Bravo-Abad and G. S. Solomon, Demonstration of Second-harmonic Generation by 4-bar-Quasi-Phasematching in a GaAs Microdisk Cavity, in *Proceedings of Nonlinear Optics*, Kohala Coast, HI, July 21-26, 2013, OSA Technical Digest, Optical Society of America, 2013, paper NF1A.1.
19. P. S. Kuo, J. S. Pelc, O. Slattery, Y.-S. Kim, M. M. Fejer and X. Tang, Efficient, Low-noise, Single-photon Frequency Conversion, in *Proceedings of CLEO: Science and Innovations*, San Jose, CA, July 9-14, 2013, OSA Technical Digest, Optical Society of America, paper JTh2A.86.
20. P. S. Kuo, J. S. Pelc, O. Slattery, Y.-S. Kim and X. Tang, Entangled Photon Generation in a Phase-modulated, Quasi-phase Matched Crystal, *Proceedings of SPIE* **8875**, 887508-1.
21. A. Lazska and Assane Gueye, Quantifying All-to-One Network Topology Robustness Under Budget Constraints, in *Proceedings of W-PIN+NetEcon 2013: The Joint Workshop on Pricing and Incentives*

- tives in Networks and Systems*, Pittsburgh, PA, June 21, 2013.
22. A. Lazska and A. Gueye, Quantifying Network Topology Robustness Under Budget Constraints, in *Proceedings of the 4th Conference on Conference on Decision and Game Theory for Security*, Dallas, TX, November 11-12, 2013.
 23. H. Mahboubi, J. Habibi, A. G. Aghdam and K. Sayrafian, Distributed Coverage Optimization in a Network of Static and Mobile Sensors, in *Proceedings of the 2013 IEEE American Control Conference (IEEE ACC 2013)*, Washington, DC, USA, June 17-19, 2013.
 24. V. Marbukh, Perron-Frobenius Measure of Systemic Risk of Cascading Overload in Complex Clouds: Work in Progress, in *Proceedings of the 6th IFIP/IEEE International Workshop on Distributed Autonomous Network Management Systems*, Ghent, Belgium, May 2013.
 25. V. Marbukh, K. Sayrafian-Pour and M. Alasti, Link Layer Adaptation in Body Area Networks: Balancing Reliability and Longevity, in *Proceedings of the 24th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2013)*, London, UK, September 8-11, 2013.
 26. W. Masoudimansour, H. Mahboubi, A. G. Aghdam and K. Sayrafian, Maximum Lifetime Strategy for Target Monitoring in Mobile Sensor Networks in Presence of Obstacles, in *Proceedings of 51st IEEE Conference on Decision and Control*, Maui, HI, December 2012.
 27. B. R. Miller and D. I. Ginev, LaTeXML 2012 - A Year of LaTeXML, in *Proceedings of the Conference on Intelligent Computer Mathematics*, Bath, UK, July 8-12, 2013, (J. Carette, et al. Eds), *Lecture Notes in Computer Science* **7961** (2013), 335-338.
 28. B. R. Miller, Three Years of DLMF: Web, Math and Search, in *Proceedings of the Conference on Intelligent Computer Mathematics*, Bath, UK, July 8-12, 2013, (J. Carette, et al. Eds), *Lecture Notes in Computer Science* **7961** (2013), 288-295.
 29. K. Mills, C. Dabrowski, J. Filliben and S. Ressler, Using Genetic Algorithms and Simulation to Search for Failure Scenarios in System Models, in *Proceedings of the Fifth International Conference on Advances in System Simulation (SIMUL 2013)*, Venice, Italy, Oct 27 - Nov 1, 2013.
 30. A. Mink and A. Nakassis, Practical Strategies for QKD Key Production, *Proceedings of SPIE* **8749** (2013), 840009-1.
 31. A. Mink and J. Bienfang, QKD on a Board Limited by Detector Rates in a Free-Space Environment, in *Proceedings of 7th International Conference on Quantum, Nano and Micro Technologies*, Barcelona, Spain, August 25-31, 2013, 28-33.
 32. R. Pozo, Efficient Q-matrix Computation for the Visualization of Complex Networks, in *Proceedings of Complex Networks Workshop*, Eighth International Conference on Signal Image Technology and Internet Based Systems, Sorrento, Italy, November 25-29, 2012, 762-767.
 33. K. Sayrafian, J. Hagedorn, W.-B. Yang and J. Terrill, Virtual Reality Platform to Study RF Propagation in Body Area Networks, in *Proceedings of the 3rd IEEE International Conference on Cognitive Info-communications (CogInfoCom'12)*, Kosice, Slovakia, December 2-5, 2012.
 34. K. Sayrafian, J. Hagedorn, M. Barbi, J. Terrill and M. Alasti, A Simulation Platform to Study Inter-BAN Interference, in *Proceedings of the 4th IEEE International Conference on Cognitive Infocommunications (CogInfoCom'13)*, Budapest, Hungary, December 2-5, 2013.
 35. O. Slattery, L. Ma, P. Kuo, Y.-S. Kim and Xiao Tang, Tunable Up-conversion Detector for Single Photon and Bi-photon Infrared Spectroscopic Applications, *Proceedings of SPIE* **8726** (2013), 87260Y-1.
 36. V. Stanford, L. Diduch, A. Fillinger and K. Sayrafian, Connecting Medical Devices Through ASTM-2761-09 Standard: Implementation Issues and Lessons Learned, in *Proceedings of the Wireless Health Conference*, Baltimore, MD, Nov. 2013.
 37. J. C. Wu, A. F. Martin, C. S. Greenberg and R. N. Kacker, Data Dependency on Measurement Uncertainties in Speaker Recognition Evaluation, in *Proceedings of the SPIE Defense, Security, and Sensing Conference* **8382**, Baltimore Maryland, April 2012, 83820D.
 38. J. C. Wu, A. F. Martin, C. S. Greenberg, R. N. Kacker and V. M. Stanford, Significance Test in Speaker Recognition Data Analysis with Data Dependency, in *Proceedings of the SPIE Defense, Security, and Sensing Conference* **8734**, Baltimore Maryland, April 2013, 87340I.
 39. W. B. Yan and K. Sayrafian, Theoretical Analysis and Modeling of Link Adaptation Schemes in Body Area Networks in *Proceedings of the 3rd International Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2012)*, Paris, France, November 21-23, 2012.

40. W. B. Yang and K. Sayrafian, Theoretical Analysis and Modeling of Link Adaptation Schemes in Body Area Networks, in *Proceedings of the 3rd International Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2012)*, Paris, France, November 21-23, 2012.
41. L. Yu, Y. Lei, R. N. Kacker and D. R. Kuhn, ACTS: A Combinatorial Test Generation Tool, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Luxembourg, March 2013, Testing Tools Track, paper 1.
42. L. Yu, M. N. Borazjany, Y. Lei, R. N. Kacker and D. R. Kuhn, An Efficient Algorithm for Constraint Handling in Combinatorial Test Generation, in *Proceedings of Sixth IEEE International Conference on Software Testing, Verification and Validation (ICST)*, Luxembourg, March 2013, Research and Industry Track, paper 3.
43. L. Yu, Y. Lei, R. N. Kacker, D. R. Kuhn, R. D. Sriram and K. G. Brady, A General Conformance Testing Framework for IEEE 11073 PHD's Communication Model, in *Proceedings of 6th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA 2013)*, Athens, Greece, May 2013, ACM 978-1-4503-1300-1/13/05.
44. L. Zappaterra, H. A. Choi, K. Sayrafian and J. I. H. Iinatti, On the Delay and Data Rate Performance of Throughput-Efficient Multi-Channel Access Algorithms in Cognitive Radio Networks, in *Proceedings of the 8th International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCON 2013)*, Washington, DC, July 8-10, 2013.
2. R. F. Boisvert (ed.), Applied and Computational Mathematics Division, Summary of Activities for Fiscal Year 2012, NISTIR 7931, April 2013.
3. A. S. Carasso, Alternative Methods of Latent Fingerprint Enhancement and Metrics for Comparing Them, NISTIR 7910, January 2013.
4. A. S. Carasso, The Use of 'Slow Motion' Lévy Stable Fractional Diffusion Smoothing in Alternative Methods of Latent Fingerprint Enhancement, NISTIR 7932, April 2013.
5. A. S. Carasso, Compensating Operators and Stable Backward in Time Marching in Nonlinear Parabolic Equations, NISTIR 7967, November 2013.
6. J. A. Warren and R. F. Boisvert (eds.), Building the Materials Innovation Infrastructure: Data and Standards, NISTIR 7898, November 2012.
7. O. Narayan, I. Saniee and V. Marbukh, Congestion Due to Random Walk Routing, arXiv:1309.0066, 2013.

Accepted

1. Z. Gimbutas and S. Veerapaneni, A Fast Algorithm for Spherical Grid Rotations and its Application to Singular Quadrature, *SIAM Journal on Scientific Computing*.
 2. W. Griffin and M. Olano, Objective Image Quality Assessment of Texture Compression, *ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games*.
 3. C. Hagwood, J. Bernal, M. Halter, J. Elliot and T. Brennan, Testing Equality of Cell Populations Based on Shape and Geodesic Distance, *IEEE Transactions on Medical Imaging*.
 4. S. P. Jordan, K. S. M. Lee and J. Preskill, Quantum Computation of Scattering in Quantum Field Theories, *Quantum Information and Computation*.
 5. J. F. Lawrence, R. N. Kacker and R. Kessel, Obtaining a Trapezoidal Distribution, *Communications in Statistics – Theory and Methods*.
 6. Y.-K. Liu, Building One-Time Memories from Isolated Qubits, *Proceedings of Innovations in Theoretical Computer Science (ITCS 2014)*.
 7. H. Mahboubi, K. Moezzi, A. G. Aghdam, K. Sayrafian and V. Marbukh, Distributed Deployment Algorithms for Improved Coverage in a Network of Wireless Mobile Sensors, *IEEE Transactions on Industrial Informatics*.
- Technical Magazine Articles**
1. I. Beichl, Hail and Farewell, *Computing in Science & Engineering* **14:6** (2012), 4.
 2. J. Kepner, T. Davis, J. Demmel, A. Edelman, H. Elman, J. Gilbert, M. Heath, D. P. O'Leary, M. Overton, Y. Saad, A. Sameh, M. Stonebraker, G. Strang, R. van de Geijn, C. Van Loan and M. Wright, The Role of Linear Algebra in the Computer Science Curriculum, *SIAM News* **46:4** (May 2013), 8.
- Technical Reports**
1. G. Alagic, S. Jeffery and S. P. Jordan, Partial-indistinguishability Obfuscation Using Braids. arXiv:1212.6458, 2012.

8. I. Matei, [A. Gueye](#) and J. S. Baras., Flow Control in Time-Varying, Random Supply Chain Networks *Journal Transportation Research Part E: Logistics and Transportation Review*.
9. [W. Mitchell](#) and [M. McClain](#), A Comparison of hp -Adaptive Strategies for Elliptic Partial Differential Equations, *ACM Transactions on Mathematical Software*.
10. [F. A. Potra](#), Interior Point Methods for Sufficient Horizontal LCP in a Wide Neighborhood of the Central Path with Best Known Iteration Complexity *SIAM Journal on Optimization*.
11. R. Sekerka, S. Coriell, and [G. McFadden](#), Morphological Stability, *Handbook of Crystal Growth*.
12. J. C. Wu, A. F. Martin and [R. N. Kacker](#), Bootstrap Variability Studies in ROC Analysis on Large Datasets, *Communications in Statistics - Simulation and Computation*.
13. D. Yeo and [F. A. Potra](#), Sustainable Design of Reinforced Concrete Structures through CO₂ Emission Optimization, Special Issue on Sustainable Building Structures, *Journal of Structural Engineering-ASCE*.
- Cement-Based Materials Cement and Concrete Composites.
10. [A. Gueye](#), A. Lazska, J. C. Walrand and V. Anantharan. A Polyhedral-Based Analysis of Nash Equilibria of Quasi-Zero-Sum Games and its Applications to Communication Network Security.
11. [S. P. Jordan](#), Strong Equivalence of Reversible Circuits is coNP-complete.
12. [N. Kaslovsky](#) and F. G. Meyer, Non-asymptotic Analysis of Tangent Space Perturbation.
13. [Y.-S. Kim](#), [O. Slattery](#), [P. S. Kuo](#) and [X. Tang](#), Two-photon Interference with Continuous-wave Multi-mode Coherent Light.
14. A. Lazska and [A. Gueye](#), Network Topology Vulnerability/Cost Tradeoff: Model, Application, and Computational Complexity.
15. A. Luna, [G. McFadden](#), [M. Aladjem](#) and K. Kohn, Predicted Role of NAD Utilization in the Control of Circadian Rhythms During DNA Damage Response.
16. I. Sahin and [A. J. Kearsley](#), Using Quadratic Functions over Lines in an Evolutionary Optimization Algorithm.
17. [B. Saunders](#), [Q. Wang](#) and B. Antonishek, Adaptive Composite B-Spline Grid Generation for Interactive 3D Visualizations.
18. M. J. Stevens, [S. Glancy](#), S. W. Nam and R. P. Mirin, Third-order Antibunching from an Imperfect Single-photon Source.
19. [A. Streib](#), [N. Streib](#), [I. Beichl](#) and F. Sullivan, Stratified Sampling for the Ising Model - A Graph Theoretic Approach.
20. [A. Streib](#), [N. Streib](#), [I. Beichl](#) and F. Sullivan, A Binomial Approximation Method for the Ising Model.
21. [A. Streib](#) and [N. Streib](#), Cycle Basis Markov Chains for the Ising Model.
22. F. Sullivan and [I. Beichl](#), Permanents, alpha-Permanents and Sinkhorn Balancing.

In Review

1. A. Boliang, [H. S. Cohl](#) and S. Weiss, A Function Selection Procedure for Determining Resonant Modes of Patch Antennas on Spherical Surfaces.
2. A. Anandkumar, D. P. Foster, D. Hsu, S. M. Kakade and [Y.-K. Liu](#), A Spectral Algorithm for Latent Dirichlet Allocation.
3. [A. S. Carasso](#), Compensating Operators and Stable Backward in Time Marching in Nonlinear Parabolic Equations.
4. [B. Cloteaux](#), M. D. LaMar, E. Moseman and [J. Shook](#), Threshold Digraphs.
5. E. Cobanera, G. Ortiz, and [E. Knill](#), The Non-Abelian Duality Problem.
6. [H. S. Cohl](#), Antiderivatives and Integral Representations of Associated Legendre Functions with Degree and Order Equal to Within a Sign.
7. [H. S. Cohl](#) and Hans Volkmer, Expansions for a Fundamental Solution of Laplace's Equation on \mathbb{R}^3 in 5-cyclidic Harmonics.
8. D. Cotrell, A. Lott and [G. McFadden](#), Boundary Slip Effects on the Stability of Spiral Poiseuille Flow.
9. C. F. Ferraris, N. Martyts, and [W. L. George](#), Development of Standard Reference Materials for

Invention Disclosures

1. A. Carasso, Enhancement and Denoising of Latent Fingerprints, May 2013.

Presentations

Invited Talks

1. R. F. Boisvert, "Society Publishing and the Fair Access Model," Dagstuhl Perspectives Workshop on the Publication Culture in Computing Research, Schloss Dagstuhl, Leibnitz-Zentrum fuer Informatik, Wadern, Germany, November 7, 2012.
2. R. F. Boisvert, "Reproducibility at ACM," Panel on Journal Policies and Experiences, Workshop on Reproducibility in Computational and Experimental Mathematics, Institute for Computational and Experimental Mathematics (ICERM), Brown University, Providence, RI, December 11, 2012.
3. R. F. Boisvert, "A Survey of Data Intensive Problems at NIST," International Workshop on Data Intensive Scientific Discovery, Shanghai, China, August 2, 2013.
4. A. S. Carasso, "Unexpected Success and Surprising Failure in Backward in Time Continuation in Linear and Nonlinear Parabolic Equations and Their Applications," International Conference on Computational Analysis of Inverse Problems and Partial Differential Equations, University of Central Florida, Orlando, FL, May 9-11 2013.
5. H. S. Cohl, "Generalizations of Generating Functions for Hypergeometric Orthogonal Polynomials," The Norbert Wiener Center Seminar, The Norbert Wiener Center for Harmonic Analysis, University of Maryland, College Park, MD, October 16, 2012.
6. H. S. Cohl, "Expansions for the Iterated Poisson Equation on d-dimensional Euclidean Space," Department of Mathematical Sciences Colloquium, George Mason University, Fairfax, VA, December 7, 2012.
7. H. S. Cohl, "Generalizations of Generating Functions for Hypergeometric Orthogonal Polynomials," Department of Mathematics, Tulane University, New Orleans, LA, February 21, 2013.
8. H. S. Cohl, "Fourier and Legendre Expansions for Green's Functions of Elliptic PDEs," Army Research Laboratory, Adelphi, MD, March 13, 2013.
9. H. S. Cohl, "Fourier and Gegenbauer Expansions of a Fundamental Solution of Laplace's Equation Riemannian Spaces of Constant Curvature," Clifford Analysis Seminar, Department of Mathematical Analysis, Ghent University, Ghent, Belgium, April 4, 2013.
10. G. Doğan, "Variational Algorithms for Fast and Robust Shape Reconstruction in Imaging," Fields Institute, University of Toronto, Canada, March 25, 2013.
11. G. Doğan, "Gradient Flows for General Curvature-dependent Surface Energies and Shape Optimization and Applications in Imaging," Summer Graduate Program on Flow, Geometric Motion, Deformation, and Mass Transport in Physiological Processes, Institute for Mathematics and its Applications, University of Minnesota, Minneapolis, MN, July 15, 2013.
12. J. T. Fong, "Quantitative NDE and Stochastic Modeling of Fatigue of Aging Structures," Department of Mechanical Engineering, Yokohama National University, Yokohama, Japan, Oct. 15, 2012.
13. J. T. Fong, "Quantitative Nondestructive Evaluation (QT-NDE): Key to Innovative Manufacturing and Aging Equipment Management," School of Mechanical and Power Engineering, East China University of Science and Technology, Shanghai, China, Oct. 19, 2012.
14. J. T. Fong, "Quantitative Nondestructive Evaluation (QT-NDE): Key to Innovative Manufacturing and Aging Equipment Management," China Standards Committee on Boilers and Pressure Vessels, Beijing, China, Oct. 22, 2012.
15. J. T. Fong, "Quantitative Nondestructive Evaluation (QT-NDE): Key to Innovative Manufacturing and Aging Equipment Management," School of Mechanical Engineering, Beijing Institute of Technology, Beijing, China, Oct. 23, 2012.
16. J. T. Fong, "Quantitative Nondestructive Evaluation (QT-NDE): Key to Innovative Manufacturing and Aging Equipment Management," School of Materials Science and Engineering, Dalian University of Technology, Dalian, China, Oct. 25, 2012.
17. J. T. Fong, "Quantitative Nondestructive Evaluation (QT-NDE): Key to Innovative Manufacturing and Aging Equipment Management," School of Mechanical Engineering, China University of Petroleum, Qingdao, China, Oct. 29, 2012.
18. J. T. Fong, "A Stochastic and Local Theory of Fatigue for Aging Pressure Vessels and Piping," International Symposium on Structural Integrity (ISSI2012), Shandong University, Jinan, China, Nov. 1, 2013.
19. J. T. Fong, "A Bayesian Stochastic Approach to Multi-Scale Modeling," Electromagnetics Division

- Seminar Series,” NIST, Boulder, CO., Feb. 26, 2013.
20. J. T. Fong, “Structural Health Monitoring of Complex Structures with Advanced NDE, Multi-Scale Modeling, and Modern Statistics,” Department of Mechanical and Industrial Engineering, University of Illinois-Chicago Circle, Chicago, IL, Apr. 18, 2013.
 21. J. T. Fong, “On the Finite Element Method-based Solutions of Electro-magnetics Problems using ABAQUS, COMSOL, and MATLAB,” Electro-magnetics Division Seminar Series, NIST, Boulder, CO., Apr. 30, 2013.
 22. J. T. Fong, “Quantitative NDE and Bayesian Fatigue Modeling: Key to Improving Reliability of Aging Structures and Components,” International Conference on Computational and Experimental Engineering and Science (ICCES’13), Bellevue, WA, May 24, 2013.
 23. J. T. Fong, “Real-Time Health Monitoring of Structures and Components with Advanced NDE, Multi-Scale Modeling, and Modern Statistics,” International Conference on Computational and Experimental Engineering and Science (ICCES’13), Bellevue, WA, May 27, 2013.
 24. J. T. Fong, “A Design of Experiments Approach to Uncertainty Assessment of NDE Field Work,” 40th Review Meeting on Quantitative Nondestructive Evaluation, Baltimore, MD, July 24, 2013.
 25. J. T. Fong, “Application of FEM- COMSOL Version 4.3b MEMS Module to the Simulation of an Electromagnetics-biased Resonator,” Applied Chemicals and Materials Division, NIST, Boulder, CO, August 8, 2013.
 26. S. Glancy, “Linear Density Matrix Estimation from Homodyne Measurements: Uncertainty Comparison,” Southwest Quantum Information Technology Network Workshop, Santa Barbara, CA, February 21, 2013.
 27. A. Gueye, “Science-Based Metrics for Network Topology Resilience against Attacks,” Mathematical Sciences Colloquium, College of Sciences, George Mason University Fairfax, VA, October 18, 2013.
 28. A. Gueye, “A Game Theoretic Framework for Evaluating Resilience of Networks Against Attacks,” Electrical and Computer Engineering Department, University of Maryland, College Park, MD, February 7, 2013.
 29. A. Gueye, “Game Theoretic Framework for Evaluating Resilience of Networks,” University of Southern California, Los Angeles, CA, January 14, 2013.
 30. A. Gueye, “Game Theoretic Framework for Evaluating Resilience of Networks,” NetEcon Meeting, University of California, Berkeley, CA, January 15, 2013.
 31. A. Gueye, “Blocking Games: A Game Theoretic Framework for Analyzing Adversarial Relationship,” TRUST Seminar Series, University of California, Berkeley, CA, January 24, 2013.
 32. A. Gueye, “Game Theoretic Framework for Evaluating Resilience of Networks,” NCD Seminar Series, University of California, Berkeley, CA, January 18, 2013.
 33. S. Jordan, “Quantum Algorithms for Quantum Field Theories,” Quantum Information Processing (QIP2013), Beijing, China, January 14, 2013.
 34. S. Jordan, “Quantum Algorithms for Quantum Field Theories,” Physics Colloquium, University of Pennsylvania, Philadelphia, PA, December 5, 2012.
 35. S. Jordan, “Super-polynomial Quantum Speedups Tutorial,” Post-quantum Cryptography Workshop, Lorentz Center, Leiden, Netherlands, November 5, 2012.
 36. S. Jordan, “Partial-indistinguishability Obfuscation using Braids,” PIQuDos Seminar, Perimeter Institute, Waterloo, Canada, April 18, 2013.
 37. S. Jordan, “Partial-indistinguishability Obfuscation using Braids” Institute for Quantum Information and Matter Seminar, Caltech, Pasadena, CA, January 8, 2013.
 38. S. Jordan, “Partial-indistinguishability Obfuscation using Braids,” Hughes Research Laboratory, Malibu, CA, January 17, 2013.
 39. D. N. Kaslovsky, “Tangent Plane Recovery and the Noise Curvature Trade Off for Local Data Parameterization,” Applied Mathematics and Statistics Colloquium, Colorado School of Mines, CO, November 16, 2012.
 40. A. J. Kearsley, “Simulation and Control of Systems Governed by PDE,” Sampoerna University, Jakarta, Indonesia, August 20, 2013.
 41. A. J. Kearsley, “Time Delay Estimation by Minimizing Differences between Linear-Phase Shifted DFTs,” University of Indonesia, August 21, 2013.
 42. P. S. Kuo, J. S. Pelc, O. Slattery, Y.-S. Kim and X. Tang, “Entangled Photon Generation in a Phase-modulated, Quasi-phase Matched Crystal,”

- SPIE Optics and Photonics 2013, San Diego, CA, August 25-29, 2013.
43. P. S. Kuo, J. Bravo-Abad, and G. S. Solomon, "Demonstration of Second-harmonic Generation by 4-bar-quasi-phaseshifting in a GaAs Micro-disk Cavity," OSA Nonlinear Optics Conference, Kohala Coast, HI, July 21-26, 2013.
 44. P. S. Kuo, "Optical Frequency Conversion and its Applications for Quantum Information," Army Research Laboratory, Adelphi, MD, January 25, 2013.
 45. Y.-K. Liu, "Building One-Time Memories from Isolated Qubits," Institute for Quantum Information and Matter Seminar, Caltech, Pasadena, CA, April 30, 2013.
 46. D. P. O'Leary, "Tracking Objects Using Wavelets and Shearlets," February Fourier Talks, University of Maryland, College Park, MD, February 2013.
 47. D. P. O'Leary, "Image Restoration and Uncertainty Quantification," 25th Biennial Numerical Analysis Conference Glasgow, Scotland, June 2013. (Plenary Talk)
 48. D. P. O'Leary, "Eckart-Young Meets Bayes: Optimal Regularized Low-Rank Inverse Approximation," International Linear Algebra Society 2013 Meeting, Providence, RI, June 2013. (Plenary Talk)
 49. N. S. Martys and W. L. George, "Computer Simulation of Suspensions: Application to Cement-based Materials," Exxon Mobil Research, Clinton, NJ, September 10, 2013.
 50. G. McFadden, "Bubble Motion and Size Variation during Thermal Migration with Phase Change," Materials Science and Technology 2013 (MS&T'13), Montreal, Canada, October 28, 2013.
 51. F. A. Potra, "Interior Point Methods for Sufficient LCP in a Wide Neighborhood of the Central Path," XXVI EURO-INFORMS 26th European Conference on Operations Research, Rome, Italy, July 1-4, 2013.
 52. S. Ressler, "Declarative 3D Graphics for the Web, Integrating X3DOM, jQuery, WebGL and HTML5," Gettysburg College, Gettysburg, PA, Oct. 10, 2013 (ACM Distinguished Speaker).
 53. B. Saunders, "Mesh Generation for Interactive 3D Graphs in the NIST Digital Library of Mathematical Functions," 19th Conference for African American Researchers in the Mathematical Sciences (CAARMS 19), San Diego, CA, July 25, 2013.
 54. K. Sayrafian, "Using Virtual Reality to Study RF Propagation, Interference & Kinetic Energy Harvesting in Body Area Networks," 8th International Conference on Body Area Networks (BodyNets 2013), September 30–October 2, 2013, Boston, MA (Keynote).
 55. K. Sayrafian, "A Virtual Reality Platform to Study RF Propagation in Body Area Networks," IEEE International Conference on Cognitive Infocommunications, December 2012.
 56. K. Sayrafian, "Body Area Networks: Standardization Activities and Technology Challenges," University of Surrey, Guildford, UK, October 10, 2012.
 57. K. Sayrafian, "Health and Medical CPS," NSF CPS PI Meeting, October 5, 2012 (Invited Panelist).
 58. J. Shook, "Threshold Digraphs," University of Colorado at Denver, Denver, CO, October 5, 2012.
 59. J. Shook, "Math at NIST," University of Colorado at Denver, Denver, CO, October 8, 2012.
 60. J. Shook, "Threshold Digraphs," Atlanta Lecture Series in Combinatorics and Graph Theory VIII, Georgia State University, Atlanta, GA, February 11, 2013.
 61. J. Shook, "Threshold Digraphs," American Mathematical Society Southeastern Spring Sectional, University of Mississippi, University, MS, March 1, 2013.
 62. J. Shook, "Math at NIST," University of Mississippi Mathematics Seminar, University, MS, March 4, 2013.
 63. A. Streib and N. Streib, "A Stratified Sampling Approach to the Ising Model," Workshop on Deep Computation in Statistical Physics, Santa Fe Institute, Santa Fe, NM, August 8, 2013.
 64. A. Streib, "Mixing times of Self-organizing Lists and Biased Permutations," IDA Center for Computing Sciences, Bowie, MD, January 30, 2013.
 65. N. Streib, "Approximating the Partition Function of the Ising Model," IDA Center for Computing Sciences, Bowie MD, January 28, 2013.
 66. N. Streib, "An Application of Graph Theory in Theoretical Physics," Discrete Mathematics Seminar, Virginia Commonwealth University, Richmond, VA, December 2013.

Conference Presentations

1. P. Bhakta, S. Miracle, D. Randall and A. P. Streib, "Mixing Times of Markov Chains for Self-Organizing Lists and Biased Permutations," SIAM Symposium on Discrete Algorithms (SODA), New Orleans, LA, January 6, 2013.
2. G. W. Bryant, N. Malkova, and J. Sims, "Electric-field Control of Exciton Fine Structure: Atomic Scale Manipulation of Exchange Splitting," American Physical Society March Meeting, Baltimore, MD, March 2013.
3. G. W. Bryant and J. S. Sims, "Magnetoexcitons in Quantum Dots: Atomistic Theory of G-Factors, Diamagnetic Shifts and Spin Mixing," International Conference on Optics of Excitons in Confined Systems, Rome, Italy, September 9-13, 2013.
4. B. Cloteaux, "Limits in Modeling Power Grid Topology," IEEE Network Science Workshop, West Point, NY, May 1, 2013.
5. H. S. Cohl, "Hypergeometric Orthogonal Polynomial Expansions," 12th International Symposium on Orthogonal Polynomials, Special Functions and Applications, Sousse, Tunisia, March 28, 2013.
6. J. Conroy, S. T. Davis, J. Kubina, Y.-K. Liu, D. P. O'Leary and J. D. Schlesinger, "Multilingual Summarization: Dimensionality Reduction and a Step Towards Optimal Term Coverage," Workshop on Multilingual Multi-document Summarization (MultiLing 2013), Sofia, Bulgaria, August 2013.
7. G. Doğan, "Shape Reconstruction from Direct and Indirect Measurements," Joint Mathematics Meetings, San Diego, CA, January 11, 2013.
8. G. Doğan, "Shape Reconstruction in Computed Tomography," Conference on Computational Analysis of Inverse Problems and Partial Differential Equations, University of Central Florida, Orlando, FL, May 9, 2013.
9. G. Doğan, "An Algorithm for Shape Detection in Computed Tomography," SIAM Conference on Computational Science and Engineering, Boston, MA, February 29, 2013.
10. G. Doğan, "Shape Reconstruction in Inverse Problems," DelMar Annual Workshop on Computational Mathematics, University of Maryland, College Park, MD, May 4, 2013.
11. M. J. Donahue, "Structure and Periodicity of Cross-tie Walls in Thin Magnetic Strips," 12th Joint MMM/Intermag Conference, Chicago, Illinois, January 16, 2013.
12. C. F. Ferraris, N. Martys and W. L. George, "Development of Standard Reference Materials for Cement-Based Materials," Fifth North American Conference on the Design and Use of Self-Consolidating Concrete (SCC2013), Chicago, IL, May 12-15, 2013.
13. A. Gueye, "Network Topology Robustness under Adversarial Environment and Budget Constraints," 4th Conference on Decision and Game Theory for Security, Dallas, TX, November 11-12, 2013.
14. A. Gueye, "A Game Theoretic Approach to Communication Security," MAA Session: Research in Applied Mathematics III, Joint Mathematics Meetings, San Diego, CA, January 9-12, 2013.
15. A. Gueye, "Cost/Benefit Analysis of Network Vulnerability Reduction: Element Hardening vs. Adding Redundancy," W-PIN+NetEcon 2013: The Joint Workshop on Pricing and Incentives in Networks and Systems, Pittsburgh, PA, June 21, 2013.
16. J. Hagedorn, K. Sayrafian, J. Terrill, "A Dynamic Human Body Computational Phantom for RF Propagation Study," 4th International Workshop on Computational Phantoms, Zurich, Switzerland, May 2013, 21-23.
17. A. Harvey, E. Simiu, F. A. Potra, K. Quinlan and N. Chokshi, "Design-basis Hurricane Winds and Missiles for Nuclear Power Plants," 22nd International Conference on Structural Mechanics in Reactor Technology (SMiRT-22), San Francisco, CA, August 18-23, 2013.
18. F. Hunt, "Characterizing Important Nodes in a Network as Effective Spreaders," SIAM Workshop on Network Science, San Diego, CA, July 8, 2013.
19. A. J. Kearsley and W. E. Wallace "Numerical Optimization of Instrument Settings in Reference Material Certification," SIAM Conference on Computational Science and Engineering, Boston, MA, March 1, 2013.
20. A. J. Kearsley, "Hierarchical Control of Mass Spectrometer Instrument Performance," 3rd IEEE International Conference on Instrumentation Control and Automation (ICA), Ungasan, Indonesia, August 29, 2013.
21. A. J. Kearsley, "Stochastic Regression Modeling of Noisy Spectra," 9th Harsh-Environment Mass Spectrometry Workshop, St. Petersburg, FL, September 15, 2013.
22. E. Knill and A. Meier, "Randomized Benchmarking," IARPA Multi-qubit Coherent Operations (MQCO) Verification and Validation of Multi-

- Qubit Systems Technical Exchange Workshop, San Diego, CA, January 2013.
23. P. S. Kuo, J. S. Pelc, O. Slattery, Y.-S. Kim, M. M. Fejer, and X. Tang, "Efficient, Low-noise, Single-Photon Frequency Conversion," Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, June 9-14, 2013.
 24. Y.-K. Liu, "Building One-time Memories from Isolated Qubits," 3rd International Conference on Quantum Cryptography (QCrypt 2013), Waterloo, Canada, August 6, 2013.
 25. Y.-K. Liu, "Evaluating the Security of Post-quantum Cryptosystems," European Telecommunications Standards Institute (ETSI) Workshop on Quantum-Safe Cryptography, Sophia-Antipolis, France, September 27, 2013.
 26. D. Lozier and A. Cuyt, "Toward an On-Demand Data Service for Special Functions," Minisymposium on Special Functions: Applications and Numerical Aspects, SIAM Annual Meeting, San Diego, CA, July 11, 2013.
 27. B. R. Miller and D. I. Ginev, "LaTeXML 2013 - A Year of LaTeXML," Conference on Intelligent Computer Mathematics, Bath, UK, July 8-12, 2013.
 28. B. R. Miller, "Three Years of DLMF: Web, Math and Search," Conference on Intelligent Computer Mathematics, Bath, UK, July 8-12, 2013.
 29. A. Mink and A. Nakassis, "Practical Strategies for QKD Key Production," SPIE Defense Security and Sensing, Baltimore, MD, April 5-9, 2013.
 30. A. Mink and J. Bienfang, "QKD on a Board Limited by Detector Rates in a Free-Space Environment," International Conference on Quantum, Nano and Micro Technologies, Barcelona, Spain, August 25-31, 2013.
 31. W. Mitchell, "Performance of *hp*-Adaptive Strategies for Elliptic Partial Differential Equations," 4th International Congress on Computational Engineering and Sciences (FEMTEC), Las Vegas, NV, May 21, 2013.
 32. D. G. Porter, "Scaling Tcl Data Structures," 20th Annual Tcl/Tk Conference, New Orleans, LA, September 26, 2013.
 33. R. Pozo, "Efficient Q-matrix Computation for the Visualization of Complex Networks," Complex Networks 2013, 8th International Conference on Signal Image Technology and Internet Based Systems, Sorrento, Italy, November 27, 2012.
 34. R. Pozo, "A Network Measure for the Analysis of Large-scale Graphs," SIAM Workshop on Network Science, San Diego, CA, July 8, 2013.
 35. R. Pozo, "Detecting Network Randomization: How Real Networks Differ from Random Graphs with the Same Joint-degree Distribution," NetSci, International School and Conference on Network Science, Copenhagen, Denmark, June 6, 2013.
 36. S. Ressler, "Web3D 2013: Scaling Up: Integrating X3DOM with Whole Body Laser Scan Data," 18th International Conference on 3D Web Technology (Web3D'13), San Sebastian, Spain, June 20 - 22, 2013.
 37. S. Ressler and K. Leber, "Web Based 3D Body Laser Scans," 4th International Conference and Exhibition on 3D Body Scanning Technologies," Long Beach CA, Nov. 19-20, 2013.
 38. K. Sayrafian, "A Dynamic Human Body Computational Phantom for RF Propagation Study," Workshop on Computational Phantoms for Radiation Protection, Imaging, and Radiotherapy, Zurich, Switzerland, May 20-22, 2013.
 39. K. Sayrafian, "Theoretical Analysis and Modeling of Link Adaptation Schemes in Body Area Networks," 3rd International Conference on Wireless Mobile Communication and Healthcare (MobiHealth 2012), Paris, France, November 21-23, 2012.
 40. K. Sayrafian, "Inter-BAN Interference Evaluation and Mitigation: A Preliminary Study," Cooperative Radio Communications for Green Smart Environments Meeting (COST IC1004), Ghent, Belgium, September 25-27, 2013.
 41. B. Saunders, "Using Adaptive Composite B-Spline Grid Generation to Enhance 3D Web Visualizations," SIAM Conference on Geometric and Physical Modeling," Denver, Colorado, November 14, 2013.
 42. B. Saunders, B. Miller, M. McClain and D. Lozier, "DLMF Live! Tables: NIST Digital Library of Mathematical Functions Tables Project," Mathematical Association of America (MAA) MD-DC-VA Section Meeting, Salisbury University, Salisbury, MD, April 13, 2013.
 43. B. Saunders, "Balancing Research Interests with Project Goals at the National Institute of Standards and Technology," MAA Session on Mathematics Experiences in Business, Industry, and Government, Joint Mathematics Meetings, San Diego, California, January 12, 2013.
 44. B. Saunders, B. Antonishek and Q. Wang, "Adaptive Composite B-Spline Grid Generation for

Interactive 3D Visualizations,” 8th International Conference on Mathematical Methods for Curves and Surfaces (MASCOT/ISGG 2012), Las Palmas de Gran Canaria, Spain, October 25, 2012.

45. K. Sayrafian-Pour, J. Hagedorn, W. Yang and J. Terrill, “A Virtual Reality Platform to Study RF Propagation in Body Area Networks,” 3rd IEEE International Conference on Cognitive Infocommunications (CogInfoCom 2012), Kosice, Slovakia, December 2-5, 2012.
46. J. Shook, “Threshold Digraphs,” Joint Mathematics Meetings, San Diego, CA, San Diego, California, January 12, 2013.
47. O. Slattery, P. Kuo, X. Tang, I. Aharonovich and S. Castelletto, “Towards Interference between Single Photons from Independent Diamond Defect and SPDC Sources,” SPIE Optics and Photonics, San Diego, CA, August 25-29, 2013.
48. A. Streib, “Clustering in Interfering Models of Binary Mixtures,” Joint Mathematics Meetings, San Diego CA, January 12, 2013.
49. N. Streib, “Dimension-Preserving Contractions and a Finite List of 3-Irreducible Posets,” Joint Mathematics Meetings, San Diego CA, January 12, 2013.

Web Services

1. Adaptive Mesh Refinement Benchmark Problems³⁰: a collection of benchmark partial differential equations for testing and comparing adaptive mesh refinement algorithms.
2. Digital Library of Mathematical Functions³¹: a repository of information on the special functions of applied mathematics.
3. Guide to Available Mathematical Functions³²: a virtual repository of mathematical software components. (dormant)
4. Matrix Market³³: a repository of matrices for testing of algorithms and software for numerical linear algebra. (dormant)
5. muMAG³⁴: a collection of micromagnetic reference problems and submitted solutions.
6. SciMark³⁵: a benchmark for scientific computing in Java. (dormant)

³⁰ <http://math.nist.gov/amr-benchmark>

³¹ <http://dlmf.nist.gov/>

³² <http://gams.nist.gov/>

³³ <http://math.nist.gov/matrixmarket/>

³⁴ <http://www.ctcms.nist.gov/mumag/mumag.org.html>

Software Released

1. ACTS³⁶: Combinatorial Test Suite Generation with Support of Constraints. Version 2.9 – Y. Lei, D. R. Kuhn and R. Kacker
2. LaTeXML³⁷: LaTeX to XML converter. Version 0.8.0 – B. Miller
3. OOF2³⁸: Finite element modeling of material microstructures. Version 2.1.8 – S. Langer
4. PHAML³⁹: Parallel Hierarchical Adaptive Multi-Level finite element program for the solution of elliptic partial differential equations. Versions 1.12.0, 1.12.1 and 1.13.0 – W. Mitchell.
5. Tcl/Tk⁴⁰: Extensible scripting language and GUI toolkit. Versions 8.4.20, 8.5.13, 8.5.14, 8.5.15, 8.6.0, 8.6.1 – D. Porter
6. Itcl: C++ inspired Object Oriented commands for Tcl. Version 4.0.0 – D. G. Porter.
7. Thread: Thread management commands for Tcl. Version 2.7.0 – D. G. Porter.
8. TDBC: Database connection commands for Tcl. Version 1.0.0 – D. G. Porter.

Conferences, Minisymposia, Lecture Series, Courses

MCS D Seminar Series

B. Cloteaux served as Chair of the ACMD Seminar Series. There were 23 talks presented during this period.

1. W. Morris (George Mason University), “Clique Number and Chromatic Number of Graphs Defined by Convex Geometries,” October 18, 2012.
2. J. Ray (Sandia National Laboratories, Livermore), “Generating Conditional Realizations of Graphs and Fields Using Markov Chain Monte Carlo,” November 5, 2012.
3. K. Hickmann (Tulane University), “Inverse Problems for Material Characterization Using Thermoacoustic Imaging,” November 16, 2012.

³⁵ <http://math.nist.gov/scimark/>

³⁶ <http://csrs.nist.gov/groups/SNS/acts/documents/comparison-report.html#acts>

³⁷ <http://dlmf.nist.gov/LaTeXML/>

³⁸ <http://www.ctcms.nist.gov/oof/>

³⁹ <http://math.nist.gov/phaml/>

⁴⁰ <http://sourceforge.net/projects/tcl/files/Tcl/8.6.1/>

4. Z. Gimbutas (New York University), "Robust High Order Integral Equation Solvers for Electromagnetic Scattering in Complex Geometries," November 29, 2012.
5. A. Carasso (ACMD), "Hazardous Continuation Backward in Time in Nonlinear Parabolic Equations, and an Experiment in Deblurring Nonlinearly Blurred Imagery," December 4, 2012.
6. A. Streib (ACMD), "Mixing Times of Self-Organizing Lists and Biased Permutations," December 12, 2012.
7. N. Streib (ACMD), "Dimension and Height for Posets with Planar Cover Graphs," January 22, 2013.
8. E. Moseman (ACMD), "The Edge of Graphicality," February 5, 2013.
9. A. Draganescu (University of Maryland Baltimore County), "Multigrid Preconditioners for Linear Systems Arising in PDE Constrained Optimization," March 5, 2013.
10. D. Cranston (Virginia Commonwealth University), "The Game of Revolutionaries and Spies on a Graph," March 12, 2013.
11. Y. Wan (University of North Texas), "Decision-making in Large-scale Dynamical Networks: Modeling, Evaluation, Estimation and Control," April 4, 2013.
12. A. Gueye (ACMD), "A Game Theoretic Framework for Evaluating Resilience of Networks against Attacks," April 16, 2013.
13. J. Chen (University of Maryland Baltimore County), "A Visualization Language," May 14, 2013.
14. G. Chen (Georgia State University), "Reed-Frost Transition on Dense Graphs," May 22, 2013.
15. S. Colbert-Kelly (ACMD), "Analysis of a Ginzburg-Landau Type Energy Model for Smectic-C* Liquid Crystal with Defects," May 28, 2013.
16. Y. Zhao (George Mason University), "On Consistency of Community Detection in Networks," June 2, 2013.
17. S. Wang (University of Houston), "Advanced Materials, Manufacturing and Design Integration for Large Offshore Wind Turbine Blades," June 12, 2013.
18. T. Kolda (Sandia National Laboratories, Livermore), "An Adaptive Power Method for the Generalized Tensor Eigenproblem," June 26, 2013.
19. S. Sarkar (Indian Statistical Institute), "Cryptanalysis of RSA Variants and Implicit Factorization," August 20, 2013.
20. M. Mascagni (Florida State University), "Monte Carlo Methods and Partial Differential Equations: Algorithms and Implications for High-Performance Computing," August 27, 2013.
21. L. Getoor (University of Maryland), "Entity-based Data Science," September 5, 2013.
22. M. Heroux (Sandia National Laboratories), "Building the Next Generation of Parallel and Resilient Applications and Libraries," September 16, 2013.
23. J. Torres-Jimenez (CINVESTAV, Mexico), "A Post-Processing Algorithm Applied to Reduce the Size of the Covering Arrays from the NIST Repository," September 19, 2013.

Courses/Shortcourses Taught

1. J. T. Fong, "Finite Element Method-based Model Simulation of Piezoelectric and Electromagnetic Phenomena," Applied Chemical and Materials Division, NIST, Boulder, CO, Feb. 25, 2013.
2. J. T. Fong, "An Introduction to Finite Element Method-based Model Simulation of Piezoelectric and Electromagnetic Phenomena," Department of Civil and Environmental Engineering, University of South Carolina, May 17, 2013.
3. J. T. Fong, "Uncertainty Quantification for Improving Engineering Reliability," Composites Design Workshop, Department of Aeronautics and Astronautics, Stanford University, July 18, 2013.
4. J. T. Fong, "Introduction to FEM-COMSOL, and its SM, AC/DC, and MEMS Modules," Electromagnetics Division, NIST, Boulder, CO., August 5-7, 2013.
5. F. Hunt, "Stochastic Processes," Graduate Course, Howard University, academic year 2012-2013.

Conference Organization

1. T. J. Burns, Mentor, Mathematical Modeling in Industry XVII – a Workshop for Graduate Students, Institute for Mathematics and Its Applications, Minneapolis, MN, August 7-16, 2013.
2. H. S. Cohl, Member, Scientific Organizing Committee, 13th International Symposium on Orthogonal Polynomials, Special Functions, and Applications (OPSFA-13), SIAM Special Interest

- Group on Orthogonal Polynomials and Special Functions, Gaithersburg, MD, 2015.
3. G. Doğan, Co-organizer, Minisymposium on Advances in Computer Algorithms for Imaging Science, SIAM Conference on Computational Science and Engineering, Boston, MA, February 25 – March 1, 2013.
 4. M. Donahue, Co-organizer Micromagnetics I Session, MMM/Intermag, Chicago, IL, January 2013.
 5. W. Griffin, Publicity Chair, ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games, Lake Buena Vista, FL, 2013.
 6. Wesley Griffin, Publicity Chair, ACM SIGGRAPH Symposium on Interactive 3D Graphics and Games, San Francisco, CA, 2014.
 7. R. N. Kacker, Co-organizer and Member, Program Committee, Second International Workshop on Combinatorial Testing (IWCT 2013), Luxembourg, March 2013.
 8. R. N. Kacker, Co-organizer, First Asian Workshop on Combinatorial Testing for Complex Computer Systems (AWCTCCS 2013), National University of Singapore, July 2013.
 9. A. Kearsley, Member, International Organizing Committee, 3rd IEEE International Conference on Instrumentation Control and Automation, Ungasan, Indonesia, 2013.
 10. P. Kuo, Member, Program Committee, CLEO S&I 4: Nonlinear Optical Technologies, Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, June 9-14, 2013.
 11. D. Lozier, Co-Chair, 13th International Symposium on Orthogonal Polynomials, Special Functions, and Applications (OPSFA-13), SIAM Special Interest Group on Orthogonal Polynomials and Special Functions, Gaithersburg, MD, 2015.
 12. V. Marbukh, Co-organizer, Bell Labs-NIST Workshop on Large-Scale Networks, Alcatel-Lucent Bell Labs, Murray Hill, NJ, October 25, 2013.
 13. B. R. Miller, Member, Program Committee, Conferences on Intelligent Computer Mathematics, Coimbra, Portugal, July 7-11, 2014.
 14. W. Mitchell, Member, Scientific Committee, International Conference of Numerical Analysis and Applied Mathematics (ICNAAM), Rhodes, Greece, September 21-27, 2013.
 15. Y. Parker and J. Terrill, Co-organizers, NIST booth, SC12, the 2012 International Conference for High Performance Computing, Networking, Storage and Analysis, Salt Lake City, Utah, November 13-19, 2012.
 16. Y. Parker and J. Terrill, Co-organizers, NIST booth, SC13, the 2013 International Conference for High Performance Computing, Networking, Storage and Analysis, Denver, CO, November 17-21, 2013.
 17. F. A. Potra, Stream Organizer, Nonlinear Optimization, XXVI EURO-INFORMS 26th European Conference on Operations Research, Rome, Italy, July 1-4, 2013.
 18. S. Ressler, Tutorial Chair, Web3D'13: 18th International Conference on 3D Web Technology, San Sebastian, Spain, June 20-22, 2013.
 19. S. Ressler, Host and Co-organizer, Web3D Tech Talk Session, 40th International Conference on Computer Graphics and Interactive Techniques, Anaheim CA, July 21-25, 2013.
 20. K. Sayrafian, Member, Technical Program Committee, 7th International Symposium on Medical Information and Communication Technology (ISMICT 2013), Tokyo, Japan, March 6-8, 2013.
 21. K. Sayrafian, Member, Technical Program Committee, 2013 IEEE International Conference on Internet of Things (iThings 2013), Beijing, China, August 20-23, 2013.
 22. K. Sayrafian, Member, Technical Program Committee, 8th International Symposium on Medical Information and Communication Technology (ISMICT 2014), Florence, Italy, April 2-4, 2014.
 23. K. Sayrafian, Member, Technical Program Committee, Symposium on Sensing, Propagation, and Wireless Networks for Healthcare Applications, IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), Singapore, April 21-24, 2014.
 24. K. Sayrafian, Member, Technical Program Committee, Seventh International Conference on Sensor Technologies and Applications (SENSORCOMM 2013), Barcelona, Spain, August 25 - 31, 2013.
 25. X. Tang, Member, Program Committee, SPIE Conference 8875: Quantum Communications and Quantum Imaging XI, SPIE Optics and Photonics, Prague, Czech Republic, 2013.

Other Professional Activities

Internal

1. I. Beichl, ITL Director, Summer Undergraduate Research Fellowship (SURF) Program.
2. R. Boisvert, NIST Scientific Computing Steering Group.
3. R. Boisvert, ITL Diversity Committee.
4. S. Glancy, NIST Boulder SURF Committee.
5. S. Glancy, ITL Diversity Committee.
6. W. Mitchell, ITL Awards Committee.
7. S. Ressler, NIST Lobby Display Advisory Council.

External

Editorial

1. I. Beichl, Editor-in-Chief, *Computing in Science & Engineering*.
2. R. Boisvert, Associate Editor, *ACM Transactions on Mathematical Software*.
3. R. Boisvert, Editor, Numerical Analysis, Mathematical Software and Computational Engineering, Finance and Science areas, Computing Research Repository (CoRR) preprint service.⁴¹
4. A. Dienstfrey, Associate Editor, *International Journal of Uncertainty Quantification*.
5. Z. Gimbutas, Member, Editorial Board, *Advances in Computational Mathematics*.
6. A. Kearsley, Member, Editorial Board, *ISRN Journal on Applied Mathematics*.
7. D. Lozier, Associate Editor, *Journal of Numerical Analysis, Industrial and Applied Mathematics*.
8. W. Mitchell, Associate Editor, *Journal of Numerical Analysis, Industrial and Applied Mathematics*.
9. D. P. O'Leary, Editor-in-Chief, *SIAM Journal on Matrix Analysis and Applications*.
10. D. P. O'Leary, Member, Editorial Board, Education Section, *SIAM Review*.
11. D. P. O'Leary, Member, Editorial Board, *SIAM Books*.

12. D. P. O'Leary, Department Editor, Your Homework Assignment, *Computing in Science & Engineering*.
13. D. P. O'Leary, Member, Editorial Board, *Computing in Science & Engineering*.
14. F. Potra, Regional Editor for the Americas, *Optimization Methods and Software*.
15. F. Potra, Associate Editor, *Journal of Optimization Theory and Applications*.
16. F. Potra, Associate Editor, *Numerical Functional Analysis and Optimization*.
17. F. Potra, Associate Editor, *Optimization and Engineering*.
18. R. Pozo, Associate Editor, *ACM Transactions on Mathematical Software*.
19. B. Saunders, Webmaster, SIAM Activity Group on Orthogonal Polynomials and Special Functions.
20. B. Saunders, OP-SF Talk listserv Moderator, SIAM Activity Group on Orthogonal Polynomials and Special Functions.
21. K. Sayrafian, Associate Editor, *International Journal on Wireless Information Networks*.

Boards and Committees

1. I. Beichl, Member, Magazine Operations Committee, IEEE Computer Society.
2. R. Bohn, Member, Cloud Computing Scoping Subcommittee, President's National Security Telecommunications Advisory Committee (NSTAC).
3. R. Bohn, Co-chair, Faster Administration of Science and Technology Education and Research (FASTER) Community of Practice, Networking and Information Technology R&D (NITRD) Program.
4. R. Boisvert, Member, International Federation for Information Processing's (IFIP) Working Group 2.5 (Numerical Software).
5. R. Boisvert, Co-chair, Publication Board, Association for Computing Machinery (ACM).
6. R. Boisvert, Member, Program Review Committee, Center for Computing Sciences, Institute for Defense Analysis.
7. R. Boisvert, Member, External Review Committee, Computer Science Department, George Washington University.
8. R. Boisvert, Member, Subcommittee on the Materials Genome Initiative, Committee on

⁴¹ <http://www.arXiv.org/>

- Technology, National Science and Technology Council.
9. A. Dienstfrey, Member, International Federation for Information Processing's (IFIP) Working Group 2.5 (Numerical Software).
 10. W. George, Member, User Advisory Council, Argonne Leadership Computing Facility.
 11. E. Knill, Member, Technical Advisory Panel, Quantum Computer Science Program, IARPA.
 12. D. Lozier, Member, Steering Committee, Painlevé Project.
 13. D. P. O'Leary, Member, Oversight Committee, Gene Golub SIAM Summer Schools.
 14. D. P. O'Leary, Member, Advisory Committee, SIAM Linear Algebra Activity Group International Summer School on Numerical Linear Algebra.
 15. V. Marbukh, Member, Network Complexity Research Group, Internet Research Task Force (IRTF).
 16. G. B. McFadden, Member, Selection Committee, SIAM Kleinman Prize.
 17. B. Miller, Member, Math Working Group, World Wide Web Consortium.
 18. D. Porter, Release Manager, Tcl Core Team.
 19. S. Ressler, Member, Declarative 3D for the Web Architecture Community Group⁴².
 20. S. Ressler, Member, Web3D Consortium.
 21. B. Saunders, Member, MAA Committee on Business, Industry and Government Mathematics.
 22. B. Saunders, Member, Advisory Group for NSF CoSMIC Scholars Program, Towson University.
 23. B. Saunders, Member, National Selection Committee Review Panel, 2013 Presidential Awards for Excellence in Mathematics and Science Teaching (PAEMST), National Science Foundation.
 24. K. Sayrafian, Member, IEEE 802.15 Working Group on Wireless Personal Area Networks.
 25. K. Sayrafian, Member, COST-IC1004, Action on Cooperative Radio Communications for Green Smart Environments, Body Area Networking Group.
 26. K. Sayrafian, Member, External Advisory Committee, Quantum Medical Device Interoperability Project (NIH funded), Medical Device "Plug-and-Play" Interoperability Program (MD PnP), Massachusetts General Hospital.
 27. K. Sayrafian, Member, Wireless Medical Technologies Working Group, National Institute for Biomedical Imaging and Bioengineering (NIBIB/NIH).
 28. J. Terrill, Member, High End Computing Research and Development and Infrastructure Interagency Working Groups, Networking and Information Technology R&D (NITRD) Program.

Thesis Direction

1. B. K. Alpert, Member, Ph.D. Thesis Committee, Ryan Lewis, Applied Mathematics, University of Colorado, Boulder. Title: *Nonlinear Approximations in Filter Design and Wave Propagation*. Completed April 9, 2013.
2. Z. Gimbutas, Member, Ph.D. Thesis Committee, Sija Hao, Applied Mathematics, University of Colorado, Boulder. Title: *Numerical Methods for Solving Linear Elliptic PDEs: Direct Solvers and High Order Accurate Discretization*. Completed 2013.
3. E. Knill, Ph.D. Thesis Adviser, Adam Meier, Physics, University of Colorado, Boulder. Title: *Randomized Benchmarking of Clifford Operators*. Completed April 19, 2013.
4. E. Knill, Ph.D. Thesis Adviser, Michael Mullan, Physics, University of Colorado, Boulder. Title: *Quantum Algorithms for Atomic Clocks*. Completed May 17, 2013.
5. E. Knill, Ph.D. Thesis Adviser, Yanbao Zhang, Physics, University of Colorado, Boulder. Title: *Analysis of Tests of Local Realism*. Completed August 20, 2013.
6. G.B. McFadden, Member, Ph.D. Thesis Committee, Augustin Luna, Biology, Boston University. Title: *Formalization of Molecular Interaction Maps in Systems Biology; Application to Simulations of the Relationship between DNA Damage Response and Circadian Rhythms*. Completed July 23, 2013.
7. B. Miller, Member, Ph.D. Thesis Committee, Deyan Ginev, Computer Science, Jacobs University Bremen. Title: *Designing Definition Discovery; Read, Recognize, Reflect, Repeat*. In process.
8. B. Miller, Member, Ph.D. Thesis Committee, Qun Zhang, Computer Science, George Washington University. Title: *Semantics-Sensitive Math-Similarity Search*. In process.
9. K. Sayrafian, Member, Ph.D. Thesis Committee, Ruijun Fu, Ye, Electrical and Computer Engineering, Worcester Polytechnic Institute. Title:

⁴² <http://www.w3.org/community/declarative3d/>

Empirical RF Propagation Modeling of Human Body Motions for Activity Classification. Completed November 28, 2012.

10. K. Sayrafian, Member, Ph.D. Thesis Committee, Yunxing Ye, Electrical and Computer Engineering, Worcester Polytechnic Institute. Title: *Comparative Performance Evaluation of RSS and TOA based Localization for Video Capsule Endoscopy inside the GI Tract*. Completed May 24, 2013.

Grants Awarded

ACMD awards a small amount of funding through the NIST Measurement Science Grants Program for projects that make direct contributions to its research programs. Often such grants support direct cooperation between an external awardee and ACMD. This year the following new cooperative agreements were initiated.

1. Society for Industrial and Applied Mathematics (SIAM): *13th International Symposium on Orthogonal Polynomials, Special Functions and Applications*, \$29,998 (1 year). PI: Dr. James Crowley.
2. Theiss Research: *Advanced Computational Tools for Shape Measurement and Analysis*, \$402,830 (3 years). PI: Dr. Gunay Doğan.
3. University of Maryland Baltimore County: *Interactive Measurement and Visualization for Heterogeneous Data Exploration in Immersive Virtual Environments*, \$438,613 (5 years). PI: Prof. Jian Chen.
4. University of Maryland: *A Science-Based Approach to Security of Complex Systems*, \$485,859 (3 years). PIs: Prof. Richard La, Dr. Assane Gueye.
5. Washington University (St. Louis): *Four-Wave Mixing in On-Chip High-Q Whispering Gallery Mode Resonators for Information Technology*, \$194,510 (3 years). PI: Prof. Lan Yang.

External Contacts

ACMD staff members make contact with a wide variety of organizations in the course of their work. Examples of these follow.

Industrial Labs

Alcatel Lucent Bell Laboratories
ActiveState
ADVR, Inc.
Cadence

CD-adapco
Feeling Structures (Brazil)
GE Healthcare
Gener8
Gulfstream Aerospace Corporation
IBM Research
KnowledgeVis, Inc.
Lepton Technology
Lockheed Martin
Mentor Graphics
Microsoft
MusixMatch
Robert Bosch GmbH (Germany)
Setterholm Consultant

Government/Non-profit Organizations

Argonne National Laboratory
Air Force Office of Scientific Research
Army Research Laboratory
Association for Computing Machinery
Center for Integration of Medicine and Innovative Technology – CIMIT
Centro Nacional de Metrologia (Mexico)
China Special Equipment Inspection and Research Institute (Beijing, China)
Electric Power Research Institute – EPRI
European Telecommunications Standards Institute
Food and Drug Administration – FDA
IDA Center for Computing Sciences
Indian Statistical Institute (India)
Institute of Physics and Chemistry of Materials (Strasbourg, France)
Intelligence Advanced Research Projects Agency – IARPA
Kentucky Science and Engineering Foundation
Lawrence Livermore National Laboratory
Leibniz Center for Informatics (Germany)
L’Istituto Nazionale di Ricerca Metrologica (Italy)
Los Alamos National Laboratory
Massachusetts General Hospital
National Security Agency – NSA
NASA Goddard Space Flight Center
NASA Ind. Verification and Validation Facility
National Center for Atmospheric Research
National Cancer Institute
National Institutes of Health – NIH
National Institute of Biomedical Imaging and Bioengineering – NIBIB
National Institute of Information and Communications Technology – NICT
National Oceanographic and Atmospheric Administration – NOAA
National Physical Laboratory (UK)
National Polytechnic Institute (Mexico)
National Renewable Energy Laboratory
National Science Foundation – NSF
Nuclear Regulatory Commission

Oak Ridge National Laboratory
 Pacific Northwest National Laboratory
 Quantum Chemistry Research Institute (Kyoto, Japan)
 Sandia National Laboratories
 SINTEF (Norway)
 Society for Industrial and Applied Mathematics –
 SIAM
 Southwest Research Institute
 Theiss Research
 US Air Force Eglin Air Force Base
 US Department of Defense
 US Department of Energy
 Web3D Consortium
 WEAR (World Engineering Anthropometry Resource)
 World Wide Web Consortium

Universities

Adam Mickiewicz University (Poland)
 Bandung Institute of Technology (Indonesia)
 Beijing Institute of Technology (China)
 Boston University
 California Institute of Technology
 Carnegie Mellon University
 China University of Petroleum (China)
 City University of Hong Kong (China)
 Concordia University (Canada)
 Dalian University of Technology (China)
 East China University of Science and Technology
 (China)
 Ecole Polytechnique de Montreal (Canada)
 Federal University of Rio Grande do Norte (Brazil)
 Federal University of Ceará (Brazil)
 Friedrich-Alexander Universität (Germany)
 George Mason University
 George Washington University
 Georgetown University
 Ghent University (Belgium)
 Humboldt University of Berlin (Germany)
 Imperial College (London)
 Indiana University
 Iowa State University
 Jacobs University Bremen (Germany)
 Johns Hopkins University Applied Physics Lab
 Institut Supérieur d'Informatique de Modélisation et de
 leurs Applications – ISIMA (France)
 National University of Singapore (Singapore)
 Nanjing University of Technology (China)
 Nanyang University (Singapore)
 New York University
 Ningbo University (China)
 Northwestern University
 Oklahoma State University
 Oregon State University
 Oslo University (Norway)

Rice University
 Royal Institute of Technology (Sweden)
 Shandong University (China)
 Shanghai University (China)
 Shippensburg University
 Stanford University
 Technical University of Denmark (Denmark)
 Technion Israel Institute of Technology (Israel)
 The College of William and Mary
 Towson University
 Tsinghua University (China)
 Tulane University
 University of Antwerp (Belgium)
 University of Belgrade (Serbia)
 University of Bergamo (Italy)
 University of British Columbia (Canada)
 University of California at Berkeley
 University of California at Irvine
 University of California San Diego
 University of Campinas (Brazil)
 University of Cantabria (Spain)
 University of Central Florida
 University of Colorado
 University of Glasgow
 University of Hong Kong (China)
 University of Illinois at Urbana-Champaign
 University of Kaiserslautern (Germany)
 University of Maryland College Park
 University of Maryland Baltimore County
 University of Melbourne (Australia)
 University of Miami
 University of Michigan
 University of Minnesota
 University of Minnesota-Duluth
 University of Montana
 University of Montreal (Canada)
 University of Nottingham (UK)
 University of Oulu (Finland)
 University of South Carolina
 University of Technology Sydney (Australia)
 University of Texas at Arlington
 University of Texas at Austin
 University of Texas El Paso
 University of Texas Pan American
 University of Tokyo (Japan)
 University of Vienna (Austria)
 University of Western Ontario (Canada)
 University of Zagreb (Croatia)
 Virginia Polytechnic Institute and State University
 Washington University
 Worcester Polytechnic Institute
 Yale University
 Yokohama National University (Japan)

Part V

Appendix



Staff

ACMD consists of full time permanent staff located at NIST laboratories in Gaithersburg, MD and Boulder, CO. This is supplemented with a variety of special appointments. The following list reflects all appointments held during any portion of the reporting period (October 2012 – December 2013). For students and interns, see Table 2, page 11. (*) Denotes staff at NIST Boulder.

Division Staff

Ronald Boisvert, *Chief*, Ph.D. (Computer Science), Purdue University, 1979
 Catherine Graham, *Secretary*
 Robert Bohn, Ph.D. (Physical Chemistry), University of Virginia, 1991
 Alfred Carasso, Ph.D. (Mathematics), University of Wisconsin, 1968
 Roldan Pozo, Ph.D. (Computer Science), University of Colorado at Boulder, 1991
 Christopher Schanzle, B.S. (Computer Science), University of Maryland Baltimore County, 1989

Mathematical Analysis and Modeling Group

Timothy Burns, *Leader*, Ph.D. (Mathematics), University of New Mexico, 1977
 *Bradley Alpert, Ph.D. (Computer Science), Yale University, 1990
 *Andrew Dienstfrey, Ph.D. (Mathematics), New York University, 1998
 Jeffrey Fong, Ph.D. (Applied Mechanics and Mathematics), Stanford University, 1966
 *Zydrunas Gimbutas, Ph.D. (Applied Mathematics), Yale University, 1999
 Fern Hunt, Ph.D. (Mathematics), New York University, 1978
 Raghuram Kacker, Ph.D. (Statistics), Iowa State University, 1979
 Anthony Kearsley, Ph.D. (Computational and Applied Mathematics), Rice University, 1996
 Geoffrey McFadden, *NIST Fellow*, Ph.D. (Mathematics), New York University, 1979
 *Agnes O’Gallagher, M.S. (Applied Mathematics), University of Colorado at Boulder, 1991
 Bert Rust, Ph.D. (Astronomy), University of Illinois at Urbana-Champaign, 1974

NRC Postdoctoral Associates

Sean Colbert-Kelly, Ph.D. (Mathematics), Purdue University, 2012
 Michael Cromer, Ph.D. (Applied Mathematics), University of Delaware, 2011

NIST-ARRA Postdoctoral Fellows

Asha Nurse, Ph.D. (Mechanical Engineering), Brown University, 2011
 Ismet Sahin, Ph.D. (Electrical and Computer Engineering), University of Pittsburgh, 2006

Faculty Appointee (Name, Degree / Home Institution)

Daniel Anderson, Ph.D. / George Mason University
 Saul Gass, Ph.D. / University of Maryland College Park
 Dianne O’Leary, Ph.D. / University of Maryland College Park
 Michael Mascagni, Ph.D. / Florida State University
 Florian Potra, Ph.D. / University of Maryland Baltimore County

Guest Researchers (Name, Degree / Home Institution)

Mirit Aladjem, Ph.D. / National Institutes of Health
 James Benson, Ph.D. / Northern Illinois University
 David Cotrell, Ph.D. / CD-Adapco
 *John Gary, Ph.D. / NIST (retired)
 David Gilsinn, Ph.D. / NIST (retired)
 *Daniel Kaslovsky, Ph.D. / University of Colorado
 Yu (Jeff) Lei, Ph.D. / University of Texas at Arlington

P. Aaron Lott, Ph.D. / Lawrence Livermore National Laboratory
 Itzel Dominquez Mendoza / Centro Nacional de Metrología, Mexico
 Bruce Murray, Ph.D. / SUNY Binghamton
 Santanu Sarkar, Ph.D. / Indian Statistical Institute
 Christoph Witzgall, Ph.D., *NIST Scientist Emeritus*

Mathematical Software Group

Michael Donahue, *Leader* Ph.D. (Mathematics), Ohio State University, 1991
 Javier Bernal, Ph.D. (Mathematics), Catholic University, 1980
 Stephen Langer, Ph.D. (Physics), Cornell University, 1989
 Daniel Lozier, Ph.D. (Applied Mathematics), University of Maryland, 1979
 Marjorie McClain, M.S. (Mathematics), University of Maryland College Park, 1984
 Bruce Miller, Ph.D. (Physics), University of Texas at Austin, 1983
 William Mitchell, Ph.D. (Computer Science), University of Illinois at Urbana-Champaign, 1988
 Donald Porter, Ph.D. (Electrical Engineering), Washington University, 1996
 Bonita Saunders, Ph.D. (Mathematics), Old Dominion University, 1985

NRC Postdoctoral Associates

Howard Cohl, Ph.D. (Mathematics), University of Auckland, 2010

Faculty Appointees (Name, Degree / Home Institution)

Frank Olver, D.Sc. / University of Maryland College Park
 G.W. Stewart, Ph.D. / University of Maryland College Park
 Abdou Youssef, Ph.D. / George Washington University

Contractors (Name, Degree / Home Institution)

Qiming Wang / Dakota Consulting

Guest Researchers (Name, Degree / Home Institution)

Gunay Dogan, Ph.D. / Theiss Research
 Adri Olde Daalhuis, Ph.D. / University of Edinburgh
 Tamara Kolda, Ph.D. / Sandia Laboratories, Livermore

Computing and Communications Theory Group

Ronald Boisvert, *Acting Leader*

Isabel Beichl, *Project Leader*, Ph.D. (Mathematics), Cornell University, 1981
 Brian Cloteaux, Ph.D. (Computer Science), New Mexico State University, 2007
 *Scott Glancy, Ph.D. (Physics), University of Notre Dame, 2003
 Barry Hershman, A.A. (Electronics Engineering), Capitol College, 1979
 Stephen Jordan, Ph.D. (Physics), Massachusetts Institute of Technology, 2008
 *Emanuel Knill, *NIST Fellow*, Ph.D. (Mathematics), University of Colorado at Boulder, 1991
 Paulina Kuo, Ph.D. (Physics), Stanford University, 2008
 Yi-Kai Liu, Ph.D. (Computer Science), University of California, San Diego, 2007
 Vladimir Marbukh, Ph.D. (Mathematics) Leningrad Polytechnic University, 1986
 Oliver Slattery, M.S. (Electrical Engineering), Johns Hopkins University, 2008
 Kamran Sayrafian-Pour, Ph.D. (Electrical and Computer Engineering), University of Maryland, 1999
 Xiao Tang, *Project Leader*, Ph.D (Physics), Chinese Academy of Sciences, 1985

NRC Postdoctoral Associates

Yvonne Kemper, Ph.D. (Mathematics), University of California at Davis, 2013
 Elizabeth Moseman, Ph.D. (Mathematics), Dartmouth College, 2007
 James Shook, Ph.D. (Mathematics), University of Mississippi, 2010

Amanda Streib, Ph.D. (Mathematics), Georgia Institute of Technology, 2012

Noah Streib, Ph.D. (Mathematics), Georgia Institute of Technology, 2012

NIST-ARRA Postdoctoral Fellows

Assane Gueye, Ph.D. (Computer Science), University of California, Berkeley, 2011

Contractors (Name, Degree / Home Institution)

Alan Mink, Ph.D. / Wagner Consulting

Faculty Appointees (Name, Degree / Home Institution)

James Lawrence, Ph.D. / George Mason University

Guest Researchers (Name, Degree / Home Institution)

*Bryan Eastin, Ph.D. / Northrup Grumman

Yong-Su Kim, Ph.D. / Pohang University of Science and Technology

Richard La, Ph.D. / University of Maryland

Francis Sullivan, Ph.D. / IDA Center for Computing Sciences

High Performance Computing and Visualization Group

Judith Terrill, Leader, Ph.D. (Information Technology), George Mason University, 1998

Yolanda Parker, Office Manager

William George, Ph.D. (Computer/Computational Science), Clemson University, 1995

Terence Griffin, B.S. (Mathematics), St. Mary's College of Maryland, 1987

Wesley Griffin, M.S. (Computer Science), University of Maryland Baltimore County, 2010

John Hagedorn, M.S. (Mathematics), Rutgers University, 1980

*Adele Peskin, Ph.D. (Chemical Engineering), University of Colorado at Boulder, 1985

Sandy Ressler, M.F.A. (Visual Arts), Rutgers University, 1980

Steven Satterfield, M.S. (Computer Science), North Carolina State University, 1975

James Sims, Ph.D. (Chemical Physics), Indiana University, 1969

Faculty Appointees (Name, Degree / Home Institution)

Marc Olano, Ph.D. / University of Maryland Baltimore County

Glossary of Acronyms

2D	two-dimensional
3D	three-dimensional
ACM	Association for Computing Machinery
ACMD	NIST/ITL Applied and Computational Mathematics Division
ACTS	Advanced Combinatorial Testing System
AIP	American Institute of Physics
AMS	American Mathematical Society
ARRA	American Recovery and Reinvestment Act
arXiv	preprint archive housed at Cornell University (http://arxiv.org/)
ASCE	American Society of Civil Engineers
ASTM	ASTM International, formerly known as the American Society for Testing and Materials
BAN	body area network
BMP	Bateman Manuscript Project
Caltech	California Institute of Technology
CCS	IDA Center for Computing Sciences
CHiMaD	Center for Hierarchical Materials Design
CI	configuration interaction
CNRS	Centre National de la Recherche Scientifique (France)
CNST	NIST Center for Nanoscale Science and Technology
CODATA	Committee on Data for Science and Technology
CPA	cryoprotective agent
CPU	central processing unit
CT	combinatorial testing
CT	computed tomography
CY	calendar year
DARPA	DOD Defense Advanced Research Projects Agency
DFT	discrete Fourier transform
DLMF	Digital Library of Mathematical Functions
DMI	Dzyaloshinskii-Moriya interaction
DNA	deoxyribonucleic acid
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOM	Document Object Model
DPD	dissipative particle dynamics
DRMF	digital repository of mathematical functions
EC	error correction
ECG	electrocardiogram
EL	NIST Engineering Laboratory
ESPCI	École Supérieure de Physique et Chimie Industrielles de la Ville de Paris (France)
ETSI	European Telecommunications Standards Institute
FASTER	Faster Administration of Science and Technology Education and Research
FDA	Food and Drug Administration
FEM	finite element method
FFT	fast Fourier transform
FPGA	field-programmable gate array
FY	fiscal year
F90gl	Fortran 90 interface to OpenGL graphics standard
GAC	Geodesic Active Contour
GAMS	Guide to Available Mathematical Software
GPU	graphics processing units
GUI	graphical user interface
HTML	hypertext markup language
HVAC	heating, ventilation and air conditioning
HVACSIM+	simulation testbed for HVAC systems

Hy-CI	Hylleraas-Configuration Interaction technique
IARPA	Intelligence Advanced Research Projects Agency
IDA	Institute for Defense Analysis
IEEE	Institute of Electronics and Electrical Engineers
IFIP	International Federation for Information Processing
IMA	Institute for Mathematics and Its Applications
IMS	Innovations in Measurement Science
INCITE	Innovative and Novel Computational Impact on Theory and Experiment (DOE Program)
IP	Internet Protocol
IPSEC	secure IP
IRTF	Internet Research Task Force
ISGG	International Society for Grid Generation
ISIMA	Institut Supérieur d'Informatique, de Modélisation et de leurs Applications (France)
ISO	International Organization for Standardization
IT	information technology
ITL	NIST Information Technology Laboratory
JILA	joint NIST-University of Colorado physics research institute
JAMA	Java Matrix package (software)
KLS	Koekoek, Lesky and Swarttouw
LaTeX	a math-oriented text processing system
LaTeXML	LaTeX to MathML translator
LDPC	low density parity check
LR	local realism
MAA	Mathematical Association of America
MALDI/TOF	matrix-assisted laser desorption/ionization time-of-flight
MathML	Mathematical Markup Language (W3C standard)
MEMS	micro-electro-mechanical system
MGI	Materials Genome Initiative
MIT	Massachusetts Institute of Technology
MKM	mathematical knowledge management
MML	NIST Material Measurement Laboratory
MPI	Message Passing Interface
MRAM	magneto-resistive random access memory
MRI	magnetic resonance imaging
MSN	mobile sensor network
muMAG	Micromagnetic Activity Group
NASA	National Aeronautics and Space Administration
NBS	National Bureau of Standards
NCAR	National Center for Atmospheric Research
NDE	non-destructive evaluation
Ngraph	Network Graph (software)
NIH	National Institutes of Health
NIR	near infrared
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal Report
NITRD	Networking and Information Technology Research and Development
NMR	nuclear magnetic resonance
NPSC	National Physical Science Consortium
NRC	National Research Council
NSF	National Science Foundation
NYU	New York University
OECD	Organization for Economic Cooperation and Development
OOF	Object-Oriented Finite Elements (software)
OOMMF	Object-Oriented Micromagnetic Modeling Framework (software)
PDE	partial differential equation
PHAML	Parallel Hierarchical Adaptive Multi Level (software)
PIV	personal identity verification

PML	NIST Physical Measurement Laboratory
PREP	Professional Research Experience Program
QDPD	quaternion-based dissipative particle dynamics
QIS	quantum information science
QKD	quantum key distribution
R&D	research and development
RF	radio frequency
SBIR	Small Business Innovative Research
SCO	NIST Standards Coordination Office
SDE	stochastic differential equation
SFI	Santa Fe Institute
SHIP	NIST Summer High School Internship Program
SIAM	Society for Industrial and Applied Mathematics
SIGGRAPH	ACM Special Interest Group on Graphics
SPIE	International Society for Optical Engineering
SRM	standard reference material
SUNY	State University of New York
SURF	Student Undergraduate Research Fellowship
SVG	scalable vector graphics
TES	transition edge sensor
TLS	transport-layer security
TNT	Template Numerical Toolkit (software)
TV	total variation
UK	United Kingdom
UMBC	University of Maryland Baltimore County
UQ	uncertainty quantification
VRML	virtual reality modeling language
W3C	World Wide Web Consortium
WebGL	Web-based Graphics Library
X3D	Extensible 3D
X3DOM	an open-source framework for integrating X3D and HTML5
XML	Extensible Markup Language