Special Projects

Digital Library of Mathematical Functions

Daniel Lozier
Ronald Boisvert
Joyce Conlon
Marjorie McClain
Bruce Fabijonas
Raghu Kacker
Bruce Miller
F.W.J. Olver
Bonita Saunders
Abdou Youssef
Charles Clark (NIST PL)
Gloria Wiersma (NIST PL)
Charles Hagwood (NIST ITL)
Nell Sedransk (NIST ITL)
Qiming Wang (NIST ITL)
Shauntia Burley (Student)
Michael Huber (Student)
Elaine Kim (Student)
Richard Askey (U. of Wisconsin, Madison)
Michael Berry (U. Bristol, UK)
Leonard Maximon (George Washington)
Morris Newman (U. California, Santa Barbara)
Ingram Olkin (Stanford)
Peter Paule (J. Kipler U., Linz, Austria)
William Reinhardt (U. Washington, Seattle)
Nico Temme (CWI, Amsterdam)

30 authors under contract

http://dlmf.nist.gov/

Mathematical functions, from the elementary ones like the trigonometric functions to the multitude of special functions, are an integral part of all modern developments in theoretical and applied science. They are used to model natural phenomena in fields from quantum theory to astrophysics, formulate problems and solutions in engineering applications, and support numerical computations. To make effective use of mathematical functions, practitioners must have ready access to a reliable catalog of their properties.

Traditionally, in all fields of science, catalogs of relevant properties have existed in the form of massive published handbooks. These are still being produced and can be found on the desks of working scientists. Recently, however, the Web is showing great promise as a more advantageous method. A big potential advantage is that scientists can begin to integrate handbook data into documents and computer programs directly, bypassing any need for time-consuming and error-prone reentry of the data and providing for much richer interconnections between data (hypertext), possibilities for annotation, and so on. Another advantage is high-resolution graphics that users can rotate and view from any angle, giving them an unprecedented way of visualizing the complex behavior of mathematical special functions.

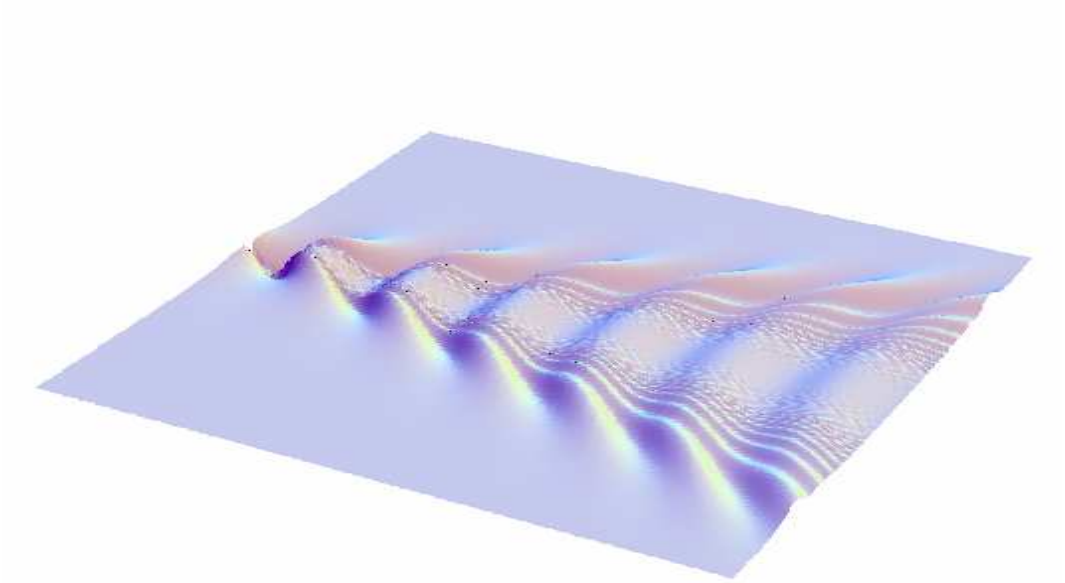
The Digital Library of Mathematical Functions has two main goals. First, to review the published literature on special functions, select the properties most relevant to current applications, and publish an up-to-date handbook of the traditional sort. The most recent comprehensive handbook was published in 1964 by the Bureau of Standards. Still in print and in widespread use, it is badly out-of-date with respect to recent mathematical research, current scientific applications of special functions, and computational methods. Second, to disseminate the same information, with important augmentations, from a Web site at NIST. The augmentations include live links to available online software and references, a math-aware search capability, a facility for downloading formulas into word processors and computer software systems, and interactive visualizations.

Substantial progress was made on both fronts in the past year. Complete drafts of all but two of the 38 planned handbook chapters have been received from authors outside NIST who are being compensated by funds from the National Science Foundation. Several chapters have been sent to

similarly compensated independent validators, and the remaining ones are scheduled for validation in the immediate future. The original plan to use HTML with GIF images for equations for the Web site has been superseded by the recent availablity of the new XML family of standards and the emerging development of tools that can put Web content into XML formats. This will yield rich improvements for math-aware search (via XQUERY) and semantic representation of mathematics in computer databases (via MathML). A major accomplishment was the project's successful construction of a translator that takes LaTeX, the mathematics word processor being used for the handbook edition, into XML/MathML. This achievement, which is at the forefront of a worldwide research effort in MKM (Mathematical Knowledge Management), was described in a keynote address and supporting technical talk at the North American MKM Workshop in January 2004, and also in an invited talk at a related workshop in Helsinki in May 2004.

Within the next year a contract with an outside publisher will be established to print, advertise and sell the handbook. The initial release of the Web site for public usage will occur simultaneously. Feedback from users is expected to suggest many avenues of enhancement for the Web site, which will continue to be an effective basis for MCSD participation in future MKM research and development activities.

This work was supported in part by the National Science Foundation (NSF) and the NIST Systems Integration for Manufacturing Applications (SIMA) Program.



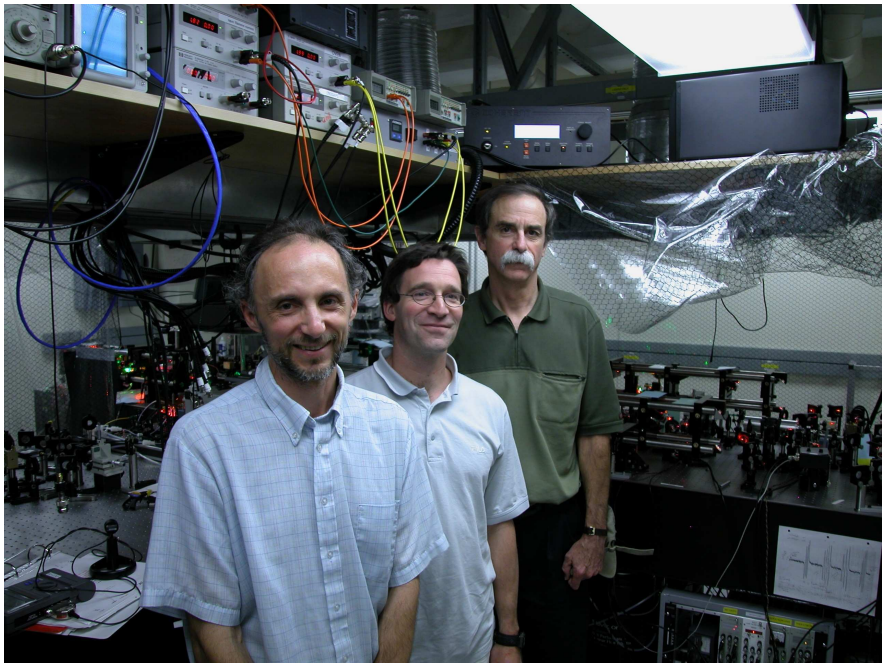
Kelvin's ship wave pattern. Many physical phenomena can be modeled very accurately with special functions. In this case the familiar wake behind a moving ship has been modeled in terms of the canonical integral associated with the cuspoid catastrophe. Catastrophe theory, begun in the 1960s, is a field of mathematics that studies and classifies phenomena characterized by sudden shifts in behavior arising from small changes in circumstances. Canonical integrals associated with different types of catastrophes are the subject of a chapter in the DLMF.

Quantum Information Theory Program

Since the mid-1960s the dimensions of transistors on microchips have halved approximately every 18 months. It is estimated that logic capacity and speed are doubling, and memory capacity is quadrupling, every three years. These rapid developments have fueled the explosive growth in information technology we have witnessed in the last 20 years. Projecting this progression into the future, a transistor will be charged with a single electron in about 15-20 years. At that point, the laws of quantum rather than classical physics will begin to dominate, requiring fundamental changes in the physical basis for computer technology if increases in computing power are to be sustained. An intriguing idea is the use of quantum states of atoms, ions, or photons themselves to store, process, and communicate information. The sometimes counterintuitive properties of quantum mechanics have led to the discovery of information processing capabilities which exceed those known classically. Among these are (a) the solution in polynomial time for problems considered exponentially difficult, such as factoring and discrete logarithms, the bases of common public-key encryption systems, and (b) communication channels secure against eavesdropping.

The NIST Physics Laboratory (PL) has a mature experimental program in quantum computing, and ITL and PL have a well established experimental program in quantum communication. MCSD is developing a program in quantum information theory to complement these efforts. This work is supported by the DARPA Quantum Information Science and Technology (QuIST) program, as well as by the NIST Competence program project entitled *Quantum Information Theory and Practice*. Work on this project centers on the development and analysis of architectures and algorithms for quantum information processing. The research being undertaken by MCSD staff is summarized below.

This work was supported in part by the NIST Competence Program and the Quantum Information Science and Technology (QUIST) Program of the Defense Advanced Projects Agency (DARPA).



Manny Knill (left) of MCSD collaborates closely with the ion trapping team led by Dave Wineland (right) of PL.

Realizing Quantum Information Processors

Emanuel Knill *David Wineland (NIST PL)*
Scott Glancy *Alan Mickelson (University of Colorado)*

Quantum information processors will solve otherwise intractable problems such as factoring large numbers and quantum physics simulation, and will greatly improve the accuracy of Monte Carlo estimates. Current quantum information processors can manipulate no more than seven quantum bits (qubits), which is sufficient for investigating quantum device behavior but not for exploiting the hoped-for computational advantages. The challenge is to obtain sufficiently capable quantum devices and to engineer appropriate architectures to build scalable quantum information processors. Quantum information is significantly more sensitive to errors than classical information. Thus one of the main problems is to obtain fault-tolerant architectures that can operate accurately at high error probabilities per device while making efficient use of available resources. MCSD's work involves

- characterizing and benchmarking quantum devices, particularly those based on ion traps and linear optics, and
- investigating fault-tolerant architectures with the goal of improving error tolerance and reducing resource requirements.

Characterization and Benchmarking. Benchmarking quantum devices involves implementing procedures and making measurement to determine how well the procedures worked. For quantum information processing, the procedures should demonstrate the functioning of fundamental algorithmic techniques used in quantum algorithms and establish the error behavior of the devices used. The most advanced scalable quantum information processors available are based on the ion trap. This year Manny Knill has collaborated closely with Dave Wineland's group in the NIST Physics Lab's Time and Frequency Division to realize three three-qubit benchmarks:

1. *Quantum teleportation*, which is one of the most versatile and useful subroutines in quantum information processors (see *Nature* v429 p737 2004);
2. *Quantum error correction*, essential for scalability (*Nature* v432 p602); and
3. Measured *quantum Fourier transform*.

The three benchmarks establish the desired quantum behavior, and provide a baseline for error behavior to be improved in future experiments. Future work includes development of procedures that provide device error information with a resolution below that implied by the error of a single measurement.

Optical quantum information processors are not sufficiently well developed to implement benchmarks with the complexity of the ion trap experiments. Therefore, the main goal in this facet of our work is to characterize the different possible approaches to implementing non-trivial tasks with optical elements. Scott Glancy recently joined the project as a NIST NRC Postdoctoral Fellow, and he and Manny Knill are now investigating how different approaches can be combined to take better advantage of the strengths of optical devices, for example, the high efficiency possible with homodyne detection. There are presently three main approaches to optical quantum computing with primarily linear optical devices: LOQC (or the KLM proposal) is based on postselection and error correction without using non-linearities; CatQC uses cat states (superpositions of two displaced Gaussian states) as a resource for computing; and the GKP proposal involves states stabilized by discrete subgroups of the quadrature displacement group. They are collaborating with Alan Mickelson at the University of Colorado, who is planning on performing experiments in optical quantum computing.

Fault-tolerant Architectures. Effective error management is the key to building practical quantum computing devices. Up to now, the most capable fault-tolerant quantum computer architectures required physical devices with error probabilities below 0.2 %. This is a difficult level for experimentalists to obtain; the best quantum devices for which error information is available have error probabilities of 3%. Manny Knill of ITL has very recently succeeded in closing this gap by designing a simple fault-tolerant architecture that can operate with devices having error probabilities above 3%. His architecture requires too large a resource overhead at such high error probabilities, but becomes relatively practical below 1%. He used several innovations to achieve this goal, most notably error-correcting teleportation, which greatly simplifies the fault-tolerant architecture while reducing the effects of errors. The error tolerance improves if the devices are able to detect their failure. There is still work to be done to reduce the resource overheads for fault-tolerant quantum information processing.

Quantum Circuit Design

Stephen Bullock
Dianne O'Leary
Gavin Brennen (NIST PL)
Igor Markov (U. of Michigan)
Vivek Shende (U. of Michigan)

Practical Top-down Approach to Quantum Circuit Synthesis. Igor Markov and Vivek Shende of the University of Michigan, working in collaboration with Stephen Bullock of ITL, have developed a new universal quantum circuit capable of implementing any unitary operator. It has a top-down structure which concentrates the circuit on the less significant qubits, and the parameters for a given unitary may be computed using standard matrix analysis software. The number of controlled-not's is only half the number of matrix coefficients. The circuit is half as large as prior art developed at the Helsinki University of Technology and for three-qubits and is half as large as a competing circuit developed at JPL. Moreover, a theoretical lower bound shows that this new universal circuit may be improved by at most a factor of two. The circuit adapts well to architectures in which only nearest-neighbor interactions are possible, i.e. spin chains. See V.V. Shende, S.S. Bullock, and I.L. Markov, quant-ph/0406176.

Constrained QR Factorization Enabling Quantum Circuit Design. Any matrix of dimension m by n can be reduced to upper triangular form by multiplying by a sequence of $mn-n(n+1)/2$ appropriately chosen rotation matrices. In this work we address the question of whether such a factorization exists when the set of allowed rotation planes is restricted. Applications to the design of 3-qubit circuits as well as to the design of quantum multi-level logics (qudits) have been studied (see below). We introduce the rotation graph as a tool to devise elimination orderings in QR factorizations. Properties of this graph characterize sets of rotation planes that are sufficient (or sufficient under permutation) and identify rotation planes to add to a deficient set. We also devise a constructive way to determine all feasible rotation sequences for performing the QR factorization using a restricted set of rotation planes. A paper by D.P. O'Leary and S. Bullock has been submitted to the *Electronic Transactions on Numerical Analysis*.

Quantum Circuits for Multi-level Logics. Dianne O'Leary and Stephen Bullock, joint with Gavin Brennen (PL), have adapted QR orthonormalization techniques from numerical linear algebra to the construction of quantum logic circuits for multi-level logics. In the usual model of quantum computing, a computation is a unitary matrix applied to a complex vector space of dimension 2^n, when n is the number of qubits. This loosely corresponds to one component per n-bit string. In a d multi-level logic, bits are replaced by dits, taking on values $0, 1, \ldots d-1$, and n quantum dits (qudits) admit computations that are $d^n \times d^n$ unitary matrices. Building a qudit quantum circuit corresponds to

splitting the unitary matrix into factors which are simple Kronecker (tensor) products. Physically, a qudit quantum system could correspond to encoding quantum data into all the hyperfine states of an atom or electron rather than simply two.

Work on qudit circuits by the group has produced three major results. First, a variant QR decomposition allows for optimal construction of one-qudit ($d \times d$) unitaries in terms of the minimum number of possible laser pulses. Second, QR arguments allow for a bootstrap argument, producing all n-qudit unitaries given one-qudit unitaries and a simple two-qudit interaction. Third, the first asymptotically optimal quantum circuit for qudits has been produced. Meaning, dimensionality arguments prove that building an n-qudit unitary requires $C\ d^{2n}$ quantum gates in a circuit. Prior circuits however required $C\ n^2\ d^{2n}$, which is asymptotically worse. Using a delicate argument involving the structure of Kronecker products, the NIST group created the first explicit quantum circuit for a $d^n \times d^n$ unitary costing only $C\ d^{2n}$ gates. This circuit is also a variant of the QR decomposition.

Small quantum circuits are hoped to make quantum computing more feasible by driving down the number of physical operations required to manipulate quantum data. In this vein, quantum multi-level logics are thought to be more efficient for packing quantum data than quantum bits in certain applications, e.g. dit-wise Fourier transforms.

See quant-ph/0410116 and quant-ph/0407223.

Entanglement Dynamics of n-qubit Computations

Stephen Bullock *Anthony Kearsley*
Dianne O'Leary *Gavin Brennen (NIST PL)*

Stephen Bullock, Gavin Brennen (PL), Dianne O'Leary, and Anthony Kearsley have been studying the entanglement dynamics of n-qubit computations. Entanglement is a quantum phenomenon which in the context of quantum computing allows a computer to manipulate superpositions (vector sums) of all n-bit strings, given the device operates on n-qubits. Prior work shows that a quantum computer incapable of creating an entangled state can never outperform a classical emulator, although how entanglement allows for quantum computer-outperformance is poorly understood.

Concurrence is one measure of entanglement, itself defined in terms of the qubit spin-flip. A quantum state which is invariant under the spin flip must be entangled. Work at NIST has discovered a new matrix decomposition of the unitary group, the concurrence canonical decomposition (CCD), which splits any quantum computation (i.e., a $2^n \times 2^n$ unitary matrix) into three factors $U = K_1 A K_2$. Only the middle factor a may alter the concurrence, so that the matrix decomposition is a tool for studying how U entangles the quantum states it processes. Results arising from this tool include the following:

- Most quantum computations produce a lot of concurrence, carrying some state with no concurrence to a state of maximal concurrence.
- Specific examples may be treated numerically in up to *10* qubits using numerical matrix analysis software. Note that *10* qubits corresponds to $2^{10} \times 2^{10} = 1024 \times 1024$ matrices.
- If the unitary has a special CCD with $K_2 = K_1^{-1}$, then eigenstates of U either have multiplicity greater than or equal to 2 or have maximal concurrence. In particular, one might envision exploiting such a Kramer's' nondegeneracy to produce highly entangled states by freezing a quantum system into such an eigenstate.
- An explicit matrix decomposition computing u exists in all cases. When the number of qubits is odd, this relies on work of Dongarra on diagonalizing Hermitian matrices with time-reversal symmetry.

See quant-ph/0309104 and quant-ph/0402051.

Other Work in Quantum Information Theory

Isabel Beichl
Stephen Bullock
David Song
Ronald Boisvert
Eite Tiesinga (NIST PL)
Francis Sullivan (IDA/CCS)

New QKD Protocols Based Upon Entanglement Swapping. David Song has developed two new cryptographic key distribution schemes based on swapping quantum entanglement. Using two Bell states, two bits of secret key can be shared between two distant parties that play symmetric and equal roles. The protocols have been shown to be robust against common eavesdropping attacks. See D. Song, *Phys. Rev. A* **69** (March 2004), p. 034301.

Optimality in Projective Measurement for Entanglement Swapping. In two partially entangled states, entanglement swapping by Bell measurement will yield the weaker entanglement of the two. This scheme is optimal because the average entanglement cannot increase under local operation and classical communication. However, for more than two states, this scheme does not always yield the weakest link. In work completed this year, David Song considered projective measurements other than Bell-type measurement and showed, numerically, that while Bell measurement may not be unique, it is indeed optimal among these projective measurements. See D. Song, *Journal of Optics B: Quantum and Semiclassical Optics* **6** (January 2004) L5-L7

Generalization to Deutsch's Algorithm Detecting Concentrated Maps. We consider an arbitrary mapping $f: \{0,\ldots,N-1\} \rightarrow \{0,\ldots,N-1\}$ for $N=2^n$. Using N calls to a classical oracle evaluating $f(x)$ and an N-bit memory, it is possible to determine whether $f(x)$ is one-to-one. For some radian angle $0 \leq \theta \leq \pi/2$ we say $f(x)$ is θ-concentrated if and only if $e^{2\pi i f(x)/N} \subset e^{i[\psi-\theta,\psi+\theta]}$ for some given ψ and any $0 \leq x \leq N-1$. We have developed a quantum algorithm that distinguishes a θ-concentrated $f(x)$ from a one-to-one $f(x)$ in $O(1)$ calls to a quantum oracle function U_f with high probability. For $0 \leq \theta \leq 0.3301$ radians, the quantum algorithm outperforms the obvious classical algorithm on average, with maximum outperformance at $\theta = (1/2)\sin^{-1}(1/\pi) \approx 0.1620$ radians. Thus, the constructions generalize Deutsch's algorithm, in that quantum outperformance is robust for (slightly) nonconstant $f(x)$. A paper by I. Beichl, S. Bullock, and D. Song has been submitted to the *NIST Journal of Research*.

A Simple Proof of the Kochen-Specker Theorem. Contextuality in a quantum mechanical system is the idea that the value of one variable depends on the context in which it is observed. Isabel Beichl and Francis Sullivan have conducted research advancing the understanding of contextuality, which has resulted in a new and simple proof of the Kochen Specker theorem, a fundamental theorem at the foundation of quantum mechanics. Their proof is understandable and hence makes one of the most fundamental ideas of quantum mechanics accessible to more researchers.

Modeling of Qubits in Optical Traps. William Mitchell is collaborating with Eite Tiesinga and other NIST PL staff using Mitchell's PHAML package to solve the Schroedinger equation for eigenvalues and eigenstates relevant to optical traps for neutral atoms. In a quantum computer, arrays of such atoms will correspond to arrays of qubits, and interactions of adjacent atoms will be used to implement elementary quantum gates. PHAML is a parallel hierarchical basis finite element solver for partial differential equations with adaptive grid refinement and multigrid linear equation solution. The computational problems in question are particularly challenging due to the large-scale variations of the eigenfunctions in small portions of the domain. Because of this, PHAML's adaptive grid refinement capabilities are critical.

This year PHAML was modified to solve equations of this form, using ARPACK as the eigensolver. The potential for the 30-node solution computed last year did not have a deep enough

well, since the physics suggests there should be about 50 nodes in the wave. At Eite's suggestion, Mitchell changed the depth of the well to one that gives a 48-node solution. This requires more processors and a longer computation time. The first attempts at solving this problem failed. Initially the 30-node solution required 1.5 million vertices and took 6 hours on 8 processors. Mitchell made several improvements to PHAML so that this now takes 7 minutes on 8 processors, a 50-fold speedup. With these improvements we are now able to produce the 48-node solution using 4.5 million vertices in 35 minutes on 32 processors.

QITAP Seminar Series. A seminar associated with the competence project Quantum Information Theory and Practice was initiated this year. The following presentations were made.

1. T. Nakassis, "Bit String Reconciliation for QKD," October 10, 2003.
2. S. Lomonaco, "Continuous Quantum Algorithms," October 30, 2003.
3. D. Song, "A QKD Protocol Based on Entanglement Swapping," November 6, 2003.
4. G. Brennen, "Universal Computation with Qudits with Applications to Multi-level Atoms," December 4, 2003.
5. S. Bullock, "Concurrence Canonical Decomposition," December 18, 2003.
6. Igor Markov (University of Michigan), Automatic Synthesis and Simulation of Quantum Circuits, January 30, 2004.
7. I. Beichl, Limits of Quantum Computation, February 5, 2004.
8. Anocha Yimsiriwattana (UMBC), Distributed Quantum Factoring Algorithm
9. Dennis Lucarelli (JHU APL), Control Theoretic Aspects of Holonomic Quantum Computation, Match 24, 2004.
10. S. Bullock, Time Reversal and the CCD Matrix Decomposition, March 25, 2004.
11. James Clemens (University of Arkansas), Partially correlated noise and quantum error correction, May 11, 2004.
12. Yaakov Weinstein (Naval Research Lab), Pseudo-Random Operators for Quantum Information Processing, September 23, 2004
13. Scott Glancy, Quantum Computation with Optical Coherent States, October 7, 2004
14. Trey Porto and Jamie Williams, Quantum Information Processing in lattices, October 21, 2004
15. S. Bullock and G. Brennen, Quantum Circuits for d-level Systems, November 7, 2004.

A Finite-Element-Analysis Code Translation Methodology for Applications in NIST World Trade Center Investigation

Jeffrey Fong
Barry Bernstein
William Mitchell
James Filliben (ITL SED)
John Gross (NIST BFRL)
Terri McAllister (NIST BFRL)
Fahim Sadek (NIST BFRL)
Monica Starnes (NIST BFRL)
Howard Baum (NIST BFRL)
Kuldeep Prasad (NIST BFRL)
Ronald Rehm (NIST BFRL)
Roland deWit (NIST MSEL)
Richard Fields (NIST MSEL)

Ala Tabiei (University of Cincinnati)
Jun Tang (University of Iowa)
Ume. Herron (Computers & Structures, Inc.)
Bob Morris (Computers & Structures, Inc.)
Iqbal Suharwardy (Computers & Structures, Inc.)
Bradley Maker (Livermore Software Tech.)
Willem Roux (Livermore Software Tech.)
Nielen Stander (Livermore Software Tech.)
Abed Khaskia (Mallet Technology)
Matt Mehalic (Mallet Technology)
Bob Rainsberger (XYZ Scientific Apps.)

Beginning on Aug. 21, 2002, NIST undertook, at the request of the Congress, a 3-part response to the Sep. 11, 2001 World Trade Center (WTC) disaster: (1) A building and fire safety investigation into the probable causes of the WTC buildings collapse; (2) A multiyear R&D program to provide the technical basis for improved building and fire codes, standards, and practices; and (3) An industry-led and NIST-assisted program to disseminate practical guidance and tools to help building owners, contractors, and designers, as well as emergency responders and regulatory authorities to better respond to future disasters.

Some of the key engineering design and analysis documents of the WTC twin towers were transmitted to NIST in the form of four computer text files, each about 100MB long, which were only executable in a commercially-available finite element analyis (FEA) software package named SAP2000. Since SAP2000 is limited in its analysis capability because it was designed to model the linear elastic response of a framed structure, NIST saw a need to translate those four text files into executables in two other software languages, namely, ANSYS and LS-DYNA, with simulation capabilities for nonlinear impact, thermal-structural interactions, buckling, creep, fracture and ultimate collapse of complex structures.

During a period of four months (Oct. 2003 - Jan. 2004), MCSD worked with researchers in NIST (BFRL and MSEL) and academia, and mathematical software developers of ANSYS, LS-DYNA, SAP2000, and a parametric FEA translator code named TrueGrid, to develop a two-option translation and verification methodology: Option-a is for a translation of SAP2000 beam elements into ANSYS (beam type 44) without cross section details. Option-b goes further by capturing all of the SAP2000 beam details into ANSYS (beam type 188). For translation from SAP2000 into LS-DYNA, only option-a was implemented, because most of the FEA analysis work by NIST and its contractors used ANSYS.

A five-criteria verification specification and a test suite of five benchmarks for the newly-developed translation methodology were introduced to facilitate the application of this methodology to WTC investigation. A MCSD working document with 22 appendices containing the results of the translation of two full floors (96A and 75B) of the WTC twin towers was completed in Jan. 2004. For further information, contact fong@nist.gov.