Mathematics Department

Professor Mark D. Meyerson
Chair

Mathematics provides a logical framework and a language indispensable to understanding the technical world in which we live. The following description summarizes the many contributions to this field of study made during the past academic year by the faculty and midshipmen majors of the Mathematics Department of the U.S. Naval Academy (USNA). The results cited reveal the great scope, diversity, and applicability of mathematics and offer glimpses of its intellectual beauty and appeal.

Several midshipmen conducted research projects as Trident Scholars, as Honors Mathematics Majors, or in specially created projects under the guidance of faculty members. Many faculty spent numerous hours serving as mentors and readers for capstone projects required of all midshipmen majors. Listed below are the three Trident Scholars with advisers in the Mathematics Department, their projects, and their Mathematics faculty mentors:

Amanda L. Donges, Quantitative Economics Major, "A Multinational Empirical Analysis of Humanitarian Assistance," Co-Adviser: Associate Professor Gary O. Fowler

Benjamin Heineike, Mathematics Major, "Modeling Morphogenesis with Reaction-Diffusion Equations Using Galerkin Spectral Methods," Advisers: Professor Reza Malek-Madani and Associate Professor Sonia M. Garcia

Noah Reddell, Electrical Engineering Major, "Covert Communication Utilizing Discretely Generated Chaos," Co-Adviser: Associate Professor Erik M. Bollt

Listed below are our seven honors Mathematics majors in the class of 2002, their projects, and their faculty mentors:

Philip Ely, "Compact Disks and Cross Interleave Reed-Solomon Codes" (Associate Professor JoAnn Turisco)

Benjamin Heineike, (also a Trident Scholar) "Simulating Pattern Formation in Reaction-Diffusion Systems" (Professor Reza Malek-Madani and Associate Professor Sonia M. Garcia)

Richard Linnell, "Elliptic Curves and Their Application to Cryptography" (Associate Professor JoAnn Turisco)

Cole Muller, "Variations on the Tower of Hanoi" (Associate Professor T. S. Michael)

Andrew Privette, "Factoring Using Lenstra's Elliptic Curve Factoring Algorithm" (Assistant Professor William Traves)

Eric Ritterman, "Variable Wave Speed and Compressional Damping" (Professor James Buchanan)

Tyler Tennille, "Construction of Codes from Algebraic Curves" (Assistant Professor William Traves)

Once again, the Mathematics Department produced a wide range of scholarly work that appeared as technical reports or as publications in refereed journals throughout the world. Dozens of articles appeared as applications of mathematics or as pure mathematical research. Topics that Mathematics Department faculty researched include: mathematics pedagogy, chaos and dynamical systems, mathematical physics and cosmology, algorithms for computers, wavelets, cryptology, ocean acoustics, navy ship degaussing, image recognition, quantum computing, and basic mathematical research in areas such as algebra, analysis, combinatorics, differential equations, matrices, number theory, operator theory, and statistics.

In addition to many independent research projects, several research projects were sponsored in whole or part by a variety of sources, such as:

Department of Health and Human Services (DHHS)
Office of Naval Research (ONR)
National Aeronautics and Space Administration (NASA)
Naval Research Laboratory (NRL)
Naval Air Warfare Center (NSWC)
Naval Surface Warfare Center (NSWC)
Naval Academy Research Council (NARC)
National Science Foundation (NSF)
National Security Agency (NSA)

During the past year, members of the Mathematics Department presented the results of their scholarly activities on over fifty occasions at professional mathematical meetings and colloquia throughout the United States and abroad. This activity, along with publication, enhances the academic stature of the Naval Academy and promotes the professional growth and reputation of those individuals involved. Through research activity, the faculty expand their intellectual horizons and stay vital in their disciplines. They contribute to the discovery of new mathematics. And they develop new materials and ideas that they can share with midshipmen students in their mathematics courses and research projects. Of special note this year, Professor Geoffrey L. Price was awarded the U.S. Naval Academy Alumni Association Civilian Faculty Award for Excellence in Research.

Sponsored Research Projects

Quantum Information Theory

Researchers: Professor B. Mitchell Baker
Sponsor: Naval Research Laboratory (NRL)

The goal of this project was to study entropy in systems of interacting qubits – for example, interacting quantum spins. The objective was to isolate an interacting subsystems (some subset of the spins) and to determine the maximum possible entropy achievable under standard time evolution: that is one-parameter unitary groups. Our method of investigation was to reduce the problem by constructing entropy equivalent classes of states, then look for a maximum in the reduced case. We were able to achieve a higher maximum for a 4-qubit system than was previously reported in the literature, but the proof is not optimal, so we have more work to do before a publication comes out of it.

Combinatorial Control of Chaos, Symbolic Dynamics, Optimal Control and Inverse Frobenius-Perron Problem

Researcher: Associate Professor Erik M. Bollt
Sponsor: National Science Foundation (NSF), Applied Mathematics Division

This project addresses global control strategies of chaotic dynamical systems. In this proposed research program, the PI will continue to develop control strategies based on transfer operator representations of the action of a chaotic dynamical system, on its invariant subspace. The objective in this research was to develop these new techniques with the primary goal being that they might naturally be used by experimentalists. To ensure such practicality, the researcher has been fostering ongoing relationships, and developing new relationships, with experimental groups.

By definition, a chaotic dynamical system is highly sensitive to small variations of states or parameters. During the last decade, a major emphasis of dynamical systems theory research has been focused on the realization that sensitive dependence provides that control of a chaotic dynamical system can be flexible and efficient. However, the majority of research has relied on local analysis of variations, which has limited application for global control objectives.

Poroelastic Media

Researcher: Professor James L. Buchanan
Sponsor: National Science Foundation (NSF)

For the past half dozen or so years the investigator and his collaborators have been studying the effects of the poroelastic parameters of a seabed on sound transmission in the ocean. The investigator is currently working on a book chapter that will summarize this research.

Human bone is a poroelastic medium consisting of an outer cortical layer surrounding a high porosity cancellous interior with an interstitial lipid fluid. An important question is can the porosity of the cancellous bone be ascertained by acoustic interrogation, thereby determining whether the bone is osteoporotic. This year the investigator worked on developing a finite elements code for calculating the acoustic field arising from cancellous bone in order to determine such parameters as its porosity, permeability, pore size and moduli of elasticity, knowledge of which would permit characterization of the health of the bone. It was found that the most important parameter, porosity, could be determined quite accurately and that some of the secondary parameters such as permeability and elastic moduli could be determined to the correct order of magnitude. These results have been submitted for publication.

The Effects of Sound on the Marine Environment (ESME)

Researcher: Professor James M. D'Archangelo
Sponsor: Naval Research Laboratory (NRL)

This work is a collaborative research initiative with the Advanced Information Technologies Branch of the Naval Research Laboratory. Our objectives are:

a. Develop a set of software tools for evaluating the impact of diverse sound sources on organisms in the underwater environment.

b. Integrate the products of the sound source/propagation loss modeling team and the biological modeling team into a simulation that incorporates environmental effects.

c. Deliver and demonstrate operation of the resulting capabilities in a decision aid that draws on shipboard tactical databases.

Two MATLAB acoustic exposure models for blue whales off the Gulf of Alaska were constructed.

a. One model was based upon the ideas of AIM (the Acoustic Integration Model developed by Marine Acoustics Inc.) By taking species-specific geographical densities and dive patterns into account, AIM calculates a root-mean-square Single Ping Equivalent (SPE) for the Received Level (RL) of the train of impulses to which animals are exposed. This calculation is a function of the duration and power of a single pulse in the pulse train, and of the total number of pulses to which the animal was exposed. The danger to the effected population is estimated using a risk function (a cumulative distribution function) to compute a risk factor, which is then normalized across the entire population of the species of interest. The risk function itself is parameterized by the minimum SPE at which animals begin to show some behavioral reaction, and a maximum SPE which is assumed to be potentially harmful.

b. The second model was based upon an acoustic dosage model similar to those used to set safety standards for human acoustic exposure.

This analysis, along with suggested improvements and directions for future research, was presented at the ESME Conference in August 2001 by Roger Hillson (Naval Research Laboratory).

Closed Loop Degaussing Using a Physical Model

Researcher: Associate Professor Gary O. Fowler
Sponsor: Naval Surface Warfare Center (NSWC)

This is a continuation of a long-standing project to measure electro-magnetic emissions of US Navy vessels. The most recent work concentrated on producing a model to align a suite of magnetic sensors using magnetic data. Each sensor was a tri-axial magnetometer whose alignment with respect to Earth's coordinate system was unknown. Directly measuring the alignment of a sensor whose dimensions are approximately 3 b 3 by 10 cm using laser sighting (or something similar) is impractical. The goal of this project was to apply a known magnetic field to the sensor, record the sensor's response and from this data calculate the alignment of the sensor. The problem was complicated by the fact that the applied field is not actually known. There was uncertainty in the magnetic source and it was impossible to produce a uniform magnetic field. Quantification of the uncertainties resulting from the only approximately known applied field was accomplished by careful measurement of a sensitive sensor that could be laser sighted and was augmented by a mathematical model of the magnetic source. Estimates of the sensor alignment and alignment uncertainty were made using principal components and regression. Finally, an investigation of the application of the sensor suit to the problem of measuring the magnetic properties of a physical model was begun.

Preliminary Measurements of Aerosol Backscatter/Extinction Ratios Using HARLIE During HARGLO-2

Researchers: Associate Professor Sonia M. F. Garcia, and
David O. Miller and Geary K. Schwemmer (NASA)
Sponsor: Code 912 – NASA / Goddard Space Flight Center

Aerosol backscatter lidar provides both high temporal and special resolution measurements of the aerosol structure of the atmosphere. Knowledge of the optical and physical properties of the aerosols are necessary in order to calculate aerosol backscatter and extinction unless the lidar observations are supplemented with an external calibration, such as the aerosol optical depth of the layer. Data collected during the HARGLO-2 wind intercomparison at the NASA Wallops Flight Facility are calibrated using aerosol optical depth measurements from an Aerosol Robotic Network (AERONET) sun-photometer.

Preliminary results from the calibration of HARLIE data using an AERONET sun photometer are presented. In general, the results seem reasonable considering the location of the data collection and the meteorological context. However, several assumptions will need to be addressed in the future. For example, the AERONET sun photometer maximum wavelength is 1020 nm. A second order polynomial fit was used to extrapolate to 1064 nm. Also, the effect of water vapor on the sun photometer measurements was not taken into account.

Representations of Finite Groups on the Riemann-Roch Space

Researchers: Professor W. David Joyner and Associate Professor William N. Traves
Sponsor: National Security Agency (NSA)

In this research, we studied the action of a finite group on the Riemann-Roch space of a curve. Our main result has the form: if G is a finite subgroup of the automorphism group of a projective curve X defined over an algebraically closed field of characteristic 0 and if D is a divisor on X fixed by G then the natural representation of G on L(D) is the direct sum of irreducible representations, all of whose dimensions are less than or equal to the size of the smallest G-orbit acting on X.

The paper "Arithmetic of Characters of Generalized Symmetric Groups," *Archiv der Mathematik*, has been accepted for publication.

On Toric Varieties and Codes

Researchers: Professor W. David Joyner and Associate Professor William N. Traves
Sponsor: National Security Agency (NSA)

This project investigates the construction and properties of Goppa codes, which are methods to encode data for fast and accurate transmission across a noisy or unstable channel. These codes are linear error-correcting codes that quite often have fast decoding algorithms. Goppa codes associated to algebraic curves are well-studied objects. One way to define the code is, roughly speaking, to evaluate a linear subspace of functions on the curve at a list of n points on the curve. This vector space of n-tuples gives rise to a Goppa code of length n. In particular, the data transmission properties of these codes are related to the algebraic and geometric properties of the curves. This project aims to extend these constructions to algebraic and projective surfaces, in particular, to toric surfaces.

Computational Aspects of Toric Varieties

Researchers: Professor W. David Joyner and H. Verrill (Louisiana State University)
Sponsor: National Security Agency (NSA)

These notes survey some basic results in toric varieties over C, with examples and applications. A computer algebra package is described which deals with both affine and projective toric varieties in any number of dimensions (written in both MAGMA and GAP). Among other things, the package implements the desingularization procedure, constructs some error-correcting codes associated with toric varieties, and computes the Riemann-Roch space of a divisor on a toric variety.

Multiplicity One for SL(2)

Researchers: Professor W. David Joyner,
Associate Professor Courtney H. Moen, and Jason Levy (University of Waterloo)
Sponsor: National Security Agency (NSA)

We applied the trace formula to the study of cuspidal automorphic representations of $SL(2,A)$ as compared with the genuine cuspidal automorphic representations of the 2-fold metaplectic cover $SL(2,A)$. The main result was a multiplicity one theorem for most automorphic representations of $SL(2)$, where A denotes the ring of adeles of a totally imaginary number field.

Nature of Spacetimes with Mild Singularities or Cauchy Horizons

Researcher: Professor Deborah A. Konkowski
Sponsor: National Science Foundation (NSF)

In this research, spacetimes with mild singularities and Cauchy horizons are being investigated. Mild singularities include quasiregular and nonscalar curvature singularities. In the case of quasiregular singularities, particle paths end suddenly with no warning from infinitely-increasing tidal forces, while in the case of nonscalar curvature singularities some, but not all, particles moving near the singularity feel infinite tidal forces. A Cauchy horizon is the boundary of the causal development of spacetime. Cauchy horizons and singularities are intimately connected, including through the cosmic censorship conjecture, which continues to be debated.

In particular, this research involves a study of (1) quantum-mechanically singular spacetimes, (2) two previously-developed stability conjectures, and (3) the global structure of mild and/or unusual singularities. This work is done in collaboration with T.M. Helliwell (Harvey Mudd College).

In the first case, following Horowitz and Marolf and work begun by T.M. Helliwell and D.A. Konkowski, classical test particles are replaced with quantum test wave packets to test the singularity structure of spacetimes which classically possess mild singularities.

In the second case, conjectures proposed by T. M. Helliwell and D. A. Konkowski to predict whether various mild singularities and Cauchy horizons are stable are being investigated further. Thus far, the singularity conjecture always holds true but the Cauchy horizon conjecture misses purely Weyl singularities that occur in the plane wave and exact mass-inflation spacetimes.

In the third case, spacetimes with nonscalar and quasiregular singularities are under investigatigation. This includes preliminary work on: (1) spacetimes with nonscalar singularities due to Siklos, (2) quasiregular singularities in the context of dislocations and disclinations and in the context of Columbeau's extended theory of distributions, and (3) the structure of some spacetimes with directional singularities.

Twin Screw Extrusion of Energetic Materials

Researchers: Assistant Professor Anastasios Liakos and Professor Reza Malek-Madani
Sponsors: Naval Surface Warfare Center (NSWC), Indian Head, MD
and Office of Naval Research (ONR)

Propellants used in weapon systems are usually extruded (*i.e.*, melted and forced through an opening) to create various shapes. It has been observed that a considerable amount of air gets trapped in the propellant during this process. The rapid changes in pressure during this process can greatly affect the temperature of the air bubbles within the propellant, bringing it close or surpassing the initiation temperature (*i.e.*, temperature at which the propellant ignites.) Through several studies done at the Naval Surface Warfare Center in Indian Head, it seems that the adiabatic compression (*i.e.*, compression at which, all thermodynamic variables, such as pressure, volume and temperature, change) of the air bubbles could play a key role in the phenomenon described above.

Vector Implementation of Godunov's Method for Euler's Equations

Researcher: Associate Professor Thomas J. Mahar
Sponsor: Naval Surface Warfare Center (NSWC), Indian Head, MD

Godunov's method for the Euler equations for fluid flow was implemented in MATLAB as vector code. The flow involves two fluids, each with its own equation of state and thermodynamic properties. The interface movement was treated as a pure advection phenomenon for the first coding. Shock fronts were captured quite well this way, while material interfaces became smeared. The very large pressure and density changes at the material interface cannot be modeled well as a pure advection process. Work on improving the performance of the code at interfaces continued, with the implementation of the level set method in conjunction with a ghost fluid approach. The results were disappointing.

Reconstruction of Phase from Amplitude only Data for Phased Array Near-Field to Far-Field Transformation and Fault Analysis

Researcher: Professor Peter A. McCoy
Sponsor: Office of Naval Research (ONR)

The purpose of this research is to apply recent wavelet-based advances by Tapan Sarkar to compute near-field measurements from amplitude only data and then apply the result to the near-field to far-field problem for a flat plate antenna. The main idea is to apply advanced methods used in other venues by Sarkar, et. al. to this problem. The advantage of the approach is that solutions are quickly and efficiently obtained using amplitude only data without having to worry about deficiencies of the other approaches such as those, which require field component sampling at the Nyquist rate. Moreover, it is easy to study antenna aperture blockage of the antenna array and to see which elements are not calibrated properly.

The Mathematics of Entanglement

Researcher: Associate Professor Robert B. Lockhart
Sponsor: Naval Research Laboratory (NRL)

This project aimed at studying mathematical properties of the sets of separable and entangled density operators for quantum systems of n-particles. The mathematics used was chiefly Hilbert space methods and differential topology. While the former is common in the field the latter is not.

Among the chief results is the construction of open neighborhoods of entangled states about maximally entangled ones. This leads to a sandwiching of all separable states. Another major result is that the set of low rank separable states forms a set of measure zero within the set of low rank states. Currently the principal investigator is attempting to show that this is false for high rank separable states. In fact, he is trying to show they contain an open ball of separable states of the same rank.

Local L2-Cohomology of Singular Spaces

Researcher: Associate Professor Caroline Grant Melles
Sponsor: Naval Academy Research Council (NARC)

This project was a continuation of joint work with Professor Pierre Milman of the University of Toronto on a problem involving the geometry of singular complex algebraic varieties. The project was motivated by a conjecture of Cheeger, Goresky, and MacPherson that the intersection cohomology of a singular algebraic variety X is isomorphic to its L2-cohomology with respect to certain types of complete Kähler metrics on the nonsingular locus of X. The conjecture is known to be true for varieties with isolated singularities and in certain other special cases. In earlier work, the investigator and Milman constructed a family of complete Kähler metrics, generalizing the metrics used for isolated singularities. Their construction is simple and explicit and uses techniques from resolution of singularities. Their objective is to investigate and describe properties of these metrics which might be used to understand their L2-cohomology.

A key feature of their construction is a careful description of properties of inverse and direct images of coherent sheaves of ideals under blow-up maps. This work led to an alternative approach to a criterion of Teissier and Lejeune for describing the sheaf of integral closures of a coherent sheaf of ideals. Integral closures of ideals occur in the construction of the authors' metrics as direct images of ideal sheaves under certain composites of blow-up maps. Sections of products of direct images are used as generating functions for complete Kähler metrics with appropriate growth rates near the singular locus of a variety. Thus, techniques for describing integral closures are useful in giving more explicit descriptions of complete Kähler metrics for singular algebraic varieties.

The investigators are writing up the results of this research to add to the following paper: "Explicit Construction of Complete Kähler Metrics of Saper Type by Desingularization," with P. Milman, (43 pages), in revision.

Matrices, Ranks, Designs, and Codes

Researcher: Associate Professor T. S. Michael
Sponsor: Naval Academy Research Council (NARC)

The row spaces over finite fields of the incidence matrices of some block designs generate error-correcting codes with pleasant, extremal properties. Recently, researchers have discovered that these extremal properties follow from basic rank inequalities, which themselves often imply the presence of a design-theoretic structure. The rank gives the dimension of the associated linear error-correcting code.

Progress was made on two fronts. First, a general duality was established between two rank inequalities for Steiner triple systems and Hadamard designs. This theorem is valid over the field with 2 elements. Second, lower bounds for the ranks of tournament matrices over finite fields are obtained. The case of equality was shown to be related to the existence of skew-Hadamard designs, a well-studied and notoriously difficult problem.

The Object-Image Equations of N Points

Researchers: Professor George C. Nakos and Dr. Robert Williams (NSWC)
Sponsor: Naval Surface Warfare Center (NSWC)

We assume that a set of three-dimensional points produces a two-dimensional image. Our goal is to describe relations between the coordinates of the object points and the image points without using the parameters of the transformation that has produced this image. These are known as object-image equations. Both the object points and the image points are determined up to a projective colineation. We base our approach on earlier work by Quan, Stiller, Asmuth, and Wan have produced a different set of object-image equations.

This is the last stage of a long project suggested by the sponsor that required several summers' work. The final form of the paper was accepted to the 8th International Conference on Applications of Computer Algebra, Volos, Greece.

The Impact of Calculus Reform on Long-term Student Performance

Researchers: Professor Howard L. Penn,
Dr. Susan Ganter (Clemson University) and Dr. Jack Bookman (Duke University)
Sponsor: National Science Foundation (NSF)

The purpose of this research project is to determine the long-term effect of the use of technology and other reformed calculus ideas on the performance of students in their upper division courses. The Naval Academy is one of several institutions participating in this study. The goals include:

a. Compare the performance of reform and traditional calculus students in courses beyond calculus

b. Examine students prior to graduation from college to determine these students' fundamental notions of calculus

c. Determine the extent to which potential employers value the ideals supported by calculus reform efforts.

Professor Howard Penn is serving as the Evaluation Fellow for the Naval Academy. His duties include:

a. Identify student subjects for interviews

b. Compile background data on student subjects

c. Compile project data

d. Analyze data

e. Develop human subjects review protocol.

Hausdorff Dimension of Harmonic Measure on Totally Disconnected Sets

Researcher: Assistant Professor Irina Popovici
Sponsor: National Science Foundation (NSF)

The goal of the project is to establish the singularity of harmonic measure and of Hausdorff measure on some totally disconnected, uniformly perfect sets (subsets of the real line or Julia sets of rational functions). The results rely on estimates of logarithmic capacities, critical values of Green's function and harmonic functions near the boundary of plane domains.

It combines potential theoretic arguments with ergodic theory and dynamical systems, and uses techniques introduced by Carleson, Jones and Wolff, Makarov and Bourgain.

Fractal sets like the ones studied in this research often appear in the analysis of the chaotic part of a dynamical system.

Shifts on Operator Algebras

Researcher: Professor Geoffrey L. Price
Sponsor: National Science Foundation (NSF)

One of the key problems in the theory of von Neumann algebras is to study and to classify the position of subfactors of a prescribed index in the hyperfinite II_1 factor R. In some ways this problem resembles the Galois theory of automorphisms of finite groups: in fact, the group-theoretic notions of index, normality, and conjugacy all have analogues in the theory of subfactors. Price has studied a family of subfactors in R on which one can define a sort of non-commutative version of the Bernoulli shift of index 2. These shifts are called Powers shifts. For each Powers shift there is a corresponding bitstream of 0's and 1's which defines the shift. The structure of the shift is reflected in certain properties possessed by the bitstream, the most accessible of which is whether or not the bitstream is eventually periodic. In fact, the bitstream is eventually periodic if and only if there is a finite positive integer k such that the kth power σ^k of the shift σ has range $\sigma^k(R)$ with nontrivial relative commutant in the hyperfinite factor R. Price has shown that all Powers shifts with relative commutant index 2 are cocycle conjugate (a natural sort of equivalence for automorphisms and endomorphisms on von Neumann algebras) and has made some progress on the higher relative commutant case. Recently, Price has discovered an unexpected connection between the conjugacy classes of Powers shifts of finite commutant index and certain classes of polynomials over the finite field of two elements, which has led to a complete classification of these shifts up to conjugacy.

Price has proved that there exist shifts of relative commutant index 2 on R which are not Powers shifts, and it is of interest to try to determine whether these new examples are cocycle conjugate to Powers shifts also of commutant index 2. The central problem in the study, though, is to try to finish the classification of the cocycle conjugacy classes of Powers shifts of higher relative commutant index.

More recently Price has turned his attention to the related subject of continuous semigroups of unital endomorphisms on operator algebras. As is true of the Powers shifts, there are analogous classification questions for these semigroups, which are called E_0–semigroups. The most fundamental examples of E_0–semigroups are those which are shifts, in the sense that the intersection of all of the ranges of the endomorphisms α_t, $t > 0$, is trivial. Very little is currently known about E_0–semigroups on II_1-factors. As a way of entering into this subject Price proposes to study a family of quantum dynamical semigroups on the free group factor F_2 on two generators and will attempt to show that these semigroups can be lifted to E_0–semigroups on the II_1-factor associated with F_2.

RAT-STATS Verification and Validation

Researcher: Professor Thomas J. Sanders
Sponsor: Department of Health and Human Services (DHHS),
Office of Inspector General, Office of Audit Services

During the period 15 June 2001 to 15 August 2001, I examined modules of the statistical software RAT-STATS for purposes of verification and validation - RAT-STATS Companion Manual, Department of Health and Human Services, Office of Inspector General, Office of Audit Services, Summer, 1996. Specific results are available on request.

The code was carefully examined to ensure that the formulas given in Reference (a) were accurately calculated. Part of this involved calling objects that I wrote in "parallel code" to verify that the results of calculations were as expected for the data inputted. Exact agreement was required in the calculation of integer values, but a tolerance of 10^{-06} = .000001 was allowed in the calculation of floating point numbers. This was to account for round-off error differences due to different coding techniques. I considered this more than adequate since results are typically reported to 2 decimals (nearest cent) and never reported to more than 3 decimals (tolerance of .0005). I paid special attention to technical calculations that each module contains, e.g., pseudo-random number generation, estimates of proportions and populations, estimates of varinces, and confidence limits.

Data sets used to examine the module calculations included ones provided by Dr. Al Kvanli and ones I created. I attempted to anticipate possible user input errors to see how the program would respond. Outputs in all formats allowed were examined to ensure that they agreed with the results of the calculations.

Modules tested and certified include the following:

a. Unrestricted Attribute Appraisal,
b. Stratified Attribute Appraisal,
c. Unrestricted Variable Appraisal,
d. Stratified Variable Appraisal,
e. Unrestricted Variable Sample Size Determination,
f. Stratified Variable Sample Size Determination, and
g. Unrestricted Attribute Sample Size Determination.

Codes on Toric Varieties

Researchers: Professor W. David Joyner and Assistant Professor William N. Traves
Sponsors: Naval Academy Research Council (NARC) and National Security Agency (NSA)

Goppa showed that interesting linear codes are associated to divisors on algebraic curves. We investigate these ideas in the context of higher-dimensional toric varieties. This project is ongoing and in its infancy.

Localization of the Hasse-Schmidt Algebra

Researcher: Assistant Professor William N. Traves
Sponsor: Naval Academy Research Council (NARC)

The behavior of the Hasse-Schmidt algebra of higher derivations under localization is studied using Andre cohomology. Elementary techniques were used to describe the Hasse-Schmidt derivations on certain monomial rings in the non-modular case. The localization conjecture was then verified for all monomial rings. Along the way, the Hasse-Schmidt derivations were interpreted as differential operators, leading to a simple description of the Steenrod operators.

Generic Initial Ideals in the Weyl Algebra

Researcher: Assistant Professor William N. Traves
Sponsor: Naval Academy Research Council (NARC)

The general linear group acts in a natural way on the Weyl algebra of differential operators on affine space. Given a generic element of the general linear group, the initial ideal of its action on a fixed ideal is well defined. As in the commutative case, these generic initial ideals have a combinatorially rigid structure. This project attempts to classify all generic initial ideals in the Weyl algebra. One expects that the structure should depend on the type of term order chosen. This project is ongoing.

Closed Loop Degaussing

Researcher: Professor John C. Turner
Sponsor: Naval Surface Warfare Center (NSWC)

The purpose of this ongoing classified project is to develop algorithms for Closed Loop Degaussing. A considerable databank has been developed on the current test platform. As we enter the third phase of research development, we consolidated the database and investigated analyzing current data in advance of the next sea trial. This analysis revealed that the data that had been collected at the three sites was inconsistent for our purposes. This inconsistency had not been observed in the earlier phases, which considered the data in less detail. To the level of detail needed for the third phase, the three sources of data are not sufficiently consistent to be used. This observation led to a review of the processing of the data. This revealed an error in processing that had not previously been noticed. The error is currently being fixed and the data re-processed.

Independent Research Projects

Graph Representations for Image Processing in Robotic Vision and Automated Fingerprint Identification

Researcher: Professor Carol G. Crawford

The author explores innovative and creative classes of graphs and their implementation in the design of algorithms for robotic vision and for classification and matching neural networks for automated fingerprint identification. The two classes of graphs include aspect graphs and sphere-of-influence graphs. The author, together with Dr. Glen Castor, was the first mathematician to explore these graphs for use in solid modeling and robotic object recognition. Collaborative work with Dr. Eric Mjolsness also provided the first application of sphere-of-influence graphs for implementation in neural network design for fingerprints.

This ongoing research extends prior work by the author in this area. This research has received prior funding from The Federal Bureau of Investigation, The Office of Naval Research, The National Institute for Standards and Technology and David Taylor Naval Research Lab.

The Elementary Theory of Groups

Researcher: Professor Anthony M. Gaglione

Remarkable ties between group theory, logic and algebraic geometry have come to light via the positive solution of the Tarski conjecture. This has led to further work on the universal theory of groups. Although this material has had a large impact on group theory, it is not as well known among group theorists as it should be. The purpose of this project was two-fold: (1) to produce an expository article in a format accessible to group theorists and to be as self-contained as possible, and (2) to continue the work on discriminating groups and squarelike groups which is an outgrowth of the above mentioned work and to tackle the most recent open questions which have arisen in this area. The principal investigator has done this work in collaboration with three other professors: B. Fine from Fairfield University, Fairfield, CT, A. Myasnikov from City College of CUNY, New York, NY, and D. Spellman from Temple University, Philadelphia, PA. As far as results and status, for number (1), the article is almost completely written and will appear in the Proceedings of St. Andrews in Oxford. This is a conference the principal investigator had attended. For (2), the work is continuing and we have assembled many answers to our previous questions.

Discriminating and Co-discriminating Groups

Researcher: Professor Anthony M. Gaglione

Discriminating and co-discriminating groups were first introduced by Baumslag, Myasnikov and Remeslennikov with an eye toward applications to the universal theory of various groups. This project is concerned with proving that a number of groups satisfy certain separation conditions which are the defining conditions for discrimination and co-discrimination. In other words, we are investigating whether certain groups are discriminating and others are non-discriminating. In order to explain what these conditions are, we need to fix some terminology. Let G and H be groups. We say that G separates H provided that for every nontrivial element h of H there exists a homomorphism $\phi_h : H \to G$ such that $\phi_h(h) \neq 1$. We say that G discriminates H provided that for every finite nonempty subset S of H of nontrivial elements there is a homomorphism $\phi_S : H \to G$ such that $\phi_S(h) \neq 1$ for all h in S. We term G discriminating provided that it discriminates every group which it separates. The theory of algebraic geometry over groups is a very useful tool for these investigations. We have been investigating several problems posed by A. Myasnikov.

General Intelligent Design Theory

Researcher: Professor Robert A. Herrmann

This is a continuous project in the theory of standard consequence operators and ultralogics. The project continues to develop or refine both standard consequence operators and ultralogics as models for the behavior of natural-systems. Most recently a new ultralogic has been developed that unifies all standard physical theories but does not carry any of the restrictions imposed upon the previous unifications.

Hopf Algebras of Trees and Quantum Field Theory

Researcher: Professor Michael E. Hoffman

In his study of renormalization in quantum field theory, Dirk Kreimer introduced a commutative Hopf algebra whose generators are rooted trees. Later, in joint work with Alain Connes, he related this Hopf algebra to another Hopf algebra arising in Connes' program of noncommutative geometry. These algebras raise many interesting algebraic and combinatorial questions. Florin Panaite claimed to prove that another Hopf algebra of trees defined earlier by Grossman and Larson is isomorphic to the graded dual of Kreimer's Hopf algebra, but his proof was incorrect. Panaite's error was to confuse two sets of multiplicities associated to pairs of rooted trees. The researcher initiated a study of the combinatorial significance of these multiplicities, with the object of relating them to earlier work.

The researcher defined linear operators on the vector space of graded trees, whose matrix coefficients are the multiplicities mentioned above, which he called the growth and pruning operators. These operators are closely related to ones defined earlier by Richard Stanley and Segey Fomin in developing the theory of "differential posets" and its generalizations. Using these operators and an appropriate inner product, the researcher achieved his goal of describing the multiplicities combinatorially, and was also able to give a corrected version of Panaite's result.

The researcher has written a paper on his work, which will be submitted for publication shortly. He has also spoken about it in a special session at a meeting of the American Mathematical Society.

Conservative Confidence for Means of Finite Populations of Nonnegatives

Researcher: Professor Harold M. Kaplan

The martingale inequality can be used for one-sided hypothesis tests of means of finite populations of nonnegatives, even when the sampling probabilities are unequal. The tests are nonasymptotic, and there is no need to estimate variance. The confidence intervals built from these tests have good numerical properties.

A Two-Sample Sign Test with Unbalanced Matching

Researcher: Professor Harold M. Kaplan

A common use of the sign test is for two samples of the same size. We match into pairs and score +1 if the number in the first sample is greater than its partner in the second sample and score -1 if less. When the two samples are slightly different in size, at least one number in the smaller sample will need to be matched with two partners from the larger sample, instead of only one partner. If ties have zero probability and no number in the smaller sample is matched with more than two partners, then the usual null hypothesis for the sign test need not be changed. Unfortunately, this is not true for three or more partners. Neither is it true if ties have nonzero probability.

Multiple Projects in the Finite Element Method

Researcher: Assistant Professor Anastasios Liakos

The researcher resubmitted the manuscript titled "Weak Imposition of Boundary Conditions in Finite Element Methods to Numerical Methods to Partial Differential Equations," and he is in the process of revising two manuscripts, "Finite Element Approximation of Viscoelastic Fluid Flow with Slip Boundary Condition" and "Multi-Level Finite Element Approximations of the Navier-Stokes Equations with Slip Boundary Condition and Large Data", that were not accepted for publication. Also, he is working with former colleagues from Clemson University on a report regarding their work on oxygen diffusion in nanocomposite materials.

In addition, he is working on two new reports: one with a colleague from the Technical University of Eindhoven, the Netherlands on the "A-posteriori error estimators for a Two-Level Finite Element Method for the Navier-Stokes Equations with Slip Boundary Condition," and the other with S. Garcia on A-posteriori error estimators for a Two-Level Finite Element Method for the Navier-Stokes Equations involving Guermond's fine scale artificial viscosity operator.

Classification of Singularities with SHEEP/CLASSI

Researcher: Professor Deborah A. Konkowski

The researcher is investigating ways to apply computer algebra programs (e.g., SHEEP/CLASSI) to the problem of singularity classification. This computer algebra research was begun during a recent sabbatical in London at Queen Mary and Westfield College with Professor Malcolm MacCallum's group and has been continued during periodic visits to London. Although it is impossible to classify topological singularities such as quasiregular singularities in this manner, scalar curvature and non-scalar curvature singularities should yield to analysis. Ways to study scalar and nonscalar curvature singularities using a complete listing of C^0- curvature invariants and frames related to parallel propagated orthonormal ones are currently under consideration.

Chain Addition Cycles

Researchers: Associate Professor Jody M. Lockhart and Professor William P. Wardlaw

Chain addition is a technique employed in cryptography for extending a short sequence of numbers, called the *seed*, to a longer sequence of pseudorandom numbers. In chain addition modulo m, the sum (modulo m) of the first two numbers of the seed is placed at the end of the seed; then the sum of the second and third numbers is placed next. This process is continued eventually using the newly generated numbers. We investigate the maximal period of chain addition cycles with seed length n (modulo m). This problem was previously studied in the case n = 2 by Green and Liebeck (Bracelets, Math Gazette, 1990) and Wall (Fibonacci series modulo m, Amer Math Monthly, 1995).

The general problem is first reduced to the case when m is a power of a prime by showing that this maximal period is submulitplicative in m. The relationship between the maximal period modulo p^k for different values of k is then investigated. It is shown that there is a positive integer r such that the periods modulo p, modulo p^2, … , modulo p^r are all equal and the period modulo p^{r+t} is p^t times the period modulo p^r for all positive integers t. The question of whether r is always 1 is investigated but not resolved.

Intrinsically Knotted Graphs

Researcher: Associate Professor T. S. Michael

Any spatial embedding of the complete graph K(7) on vertices has the property that one of its Hamilton cycles must be knotted. We seek other minimal examples of intrinsically knotted graphs. This joint research is in progress.

Games on Oriented Graphs

Researchers: Associate Professor T. S. Michael and Thomas Quint

This research investigates a zero-sum, two-person game defined by an oriented graph. Researchers have recently shown that if the oriented graph is a tournament, then the optimal strategy is unique. We obtain some sufficient conditions for non-uniqueness of the optimal strategies for more general classes of oriented graphs.

Various Problems in Combinatorics, Number Theory, and Representation Theory

Researcher: Associate Professor Courtney H. Moen

The researcher is working on various problems in combinatorics, number theory and representation theory. In particular, he has just recently started working with Associate Professor T.S. Michael on various generalizations of the Tower of Hanoi problem.

Functions in Generalized Moulis Classes

Researcher: Associate Professor E. John Moulis

Let N be the set of all (complex-valued) functions analytic in the unit disk |z| < 1, having the form f(z) = z + sum[a(n)*z^n, n=2..infinity]. We continue the study of the class U(k,c,b,L) of generalized Pinchuk functions consisting of those functions in N which, with J(f) = 1 – 1/c +(z/c)*(f'/f). z = r*e^(it), r in [0,1), t in [0,2*Pi), c a non-zero complex number and L in (-Pi/2,Pi/2), b in [0,1) and k greater than or equal to 2, we have, using MAPLE syntax,

Int [|Re{e^(it)*J(f) – b*cos(L)|,t,t=0..2*Pi] < k*(Pi)*(1-b)cos(L).

When z*f '(z) is in U(k,c,b,L), f is said to belong to a generalized Moulis class V(k,c,b,L). This researcher introduced the class V(k,0,0,L) in his Ph. D. thesis. We try to find sharp bounds in terms of the real parameters k, b and L and the complex number c, for the geometric mapping properties of functions in these classes, including distortion bounds on |f(z)| and |f '(z)| , rotation bounds on |arg(f ' (z)| as well as bounds on the moduli of the series coefficients a(n).

Mathematical Foundation for Empirical Mode Decomposition

Researchers: Associate Professor John F. Pierce,
Jorge E. Pinzon, SSAI, Norden Huang, NASA-GSFC,
Ronald M. Devore, University of South Carolina.

Utilizing the Hilbert transform, Dr. N. Huang developed a remarkably successful and robust empirical methodology to extract multi-resolution information from time series data in a nonlinear (signal-dependent) manner (*Proc. R. Soc. Lond. A.* (1998) 454, 903-995; *Annu. Rev. Fluid Mech.* 1999, 31:417-57). By an empirical "sifting" process, the method resolves the signal into a finite sum of intrinsic modes, each of which isolate features of the signal at a particular time scale. In contrast to most methods of representing signals, the intrinsic modes are not a basis set of functions imposed externally on the signal, and whose features are known prior to considering the signal. Rather, they emerge from the signal, are peculiar to it, and their features are not known prior to considering the signal.

As successful as the technique has been in its empirical applications, there are issues about the rational basis for its success, and concern for delineating its scope of validity. For example, are there time series sufficiently complex that sifting will cycle toward, but not converge to a specific intrinsic mode? Are there attributes delineating an intrinsic mode that are independent of the context, by which someone "untutored" in the particular signal would infer, correctly, the shifting process delivers an intrinsic mode? Are there formal results that affirm that iterative shifting of a signal will produce a finite set of intrinsic modes and a single, residual trend?

Wavelet Compression with Redundancy for Wireless Communication

Researchers: Dr. Ron DeVore, Dr. Robert Sharpley, University of South Carolina, and Associate Professor John F. Pierce

Wireless communication places constraints upon applications that include dynamically varying bandwidth availability, noisy and temporary loss of channels, multi-path reflections, and true channel throughput issues that render current encoder/decoder technologies inapplicable.

The inherent scalability and the progressive features of wavelet-based compression and encoding make it attractive to exploit the full potential of delivering information within the parameters of wireless communication. Wavelet-based applications revolutionized encoder decoder technology in the tethered environment of high-performance Ethernet and modem networks. Here one could handle encoded data within the optimal conditions of large bandwidth and few interference issues. In the presence of large bandwidth, data error handling could be treated straightforwardly. Wavelet-based encoding activity could be directed towards quality and performance, with little activity directed toward issues arising in the transport of data.

The opposite is the case with wireless communication. Because of the severely limited bandwidth, and because of the noisy channels for communication, data error handling becomes an intrinsic part of compression, encoding, and decoding. Compression that over-represents a signal (redundant information) provides a means by which information can be conveyed, though data is lost in transmission. We examine the issues of how wavelet-based frames can provide redundant compression at the applications layer that is consonant with the data error handling protocols operating at the physical layers of the ISO.

Geometric Properties of Julia Sets

Researcher: Assistant Professor Irina Popovici

The researcher is interested in describing the polynomials whose domains of attraction to infinity satisfy Holder-like decaying bounds for the Green function near the boundary. For real quadratic polynomials this can be characterized in terms of expansion near periodic points and in terms of derivative growth along the critical orbit.

Combinatorics of Clique Sequences

Researchers: Assistant Professor William N. Traves and Associate Professor T. S. Michael

An n-clique in a graph G is a complete subgraph of G with n vertices. We are interested in the structure of the graded poset of cliques in a graph. This interest takes many forms and avenues, including the study of the rank generating polynomial (the clique polynomial) and the Hopf-algebra structure of these posets. This project is ongoing.

Commutative Algebra and Graph Theory

Researchers: Assistant Professor William N. Traves and Sara Faridi, George Washington University

There are many commutative ideals that are naturally associated to graphs. Perhaps the best-studied is the ideal associated to a simplicial complex. Another interesting ideal is the “edge ideal” of a graph. This is the topic of a recent book by R. Villareal. Our aim in this project is to extend some of these new ideas and methods to hypergraphs, producing a new series of results about simplicial complexes. This project complements previous work by Sara Faridi.

Derived Functors of Differential Operators on Stanley-Reisner Rings

Researcher: Assistant Professor William N. Traves

Stanley-Reisner rings are closely connected with simplicial complexes. I studied differential operators on such rings in my Ph.D. thesis. In this project I study the derived functors of differential operators on these rings.

Local Cohomology for Stanley-Reisner Rings

Researcher: Assistant Professor William N. Traves

Lyubeznick studied the local cohomology of smooth varieties (regular rings). I seek to generalize his work to the class of Stanley-Reisner rings – rings with very mild singularities.

Computational Algorithms in Algebraic Number Theory

Researcher: Associate Professor JoAnn S. Turisco

This project is a continuation of my previous work which involves the use of Maple and Mathematica for computations, and to generate examples with the goal of making progress towards the solution of some open and difficult problems in algebraic number theory.

One part of this work is the explicit computation of forms associated to smooth maps between Euclidean spaces. These computations, which involve the determination of eigenvalues of large matrices whose elements are multivariable polynomials, have produced generalized hypergeometric functions.

I have continued my study of the problem of the existence of normed bilinear maps from an algebraic viewpoint, using Jordan algebras and triple systems. Examples are generated with Maple and Mathematica by associating to each map a family of rectangular matrices which satisfy certain idempotent and anti-commutative properties.

My work also involves using Maple and Mathematica in determining prime numbers and class numbers of certain algebraic number fields.

Matrix Factorization of Polynomials

Researcher: Professor William P. Wardlaw

Two methods of factoring polynomials using matrices are being studied. The first method applies to factoring cyclotomic polynomials over finite fields. Consider the cyclotomic polynomial $c_n(x)$ over the q element field $\mathbf{F}_q$ in the case that n and q are relatively prime. Find the smallest positive integer d such that n divides $q^d - 1$. (Euler's Totient Theorem guarantees that such a d exists.) It turns out that each of the irreducible factors of $c_n(x)$ is of degree d, and that $c_n(x)$ factors completely, or *splits*, over the field $\mathbf{F}_r$ with $r = q^d$. Find an irreducible polynomial over $\mathbf{F}_q$ of degree d. Then the companion matrix M of this polynomial can be considered to be an element of $\mathbf{F}_r$, which is isomorphic to the algebra $\mathbf{F}_q[M]$ generated by M over field $\mathbf{F}_q$. Some linear combination C of M with order $r-1$ will be a *cyclic generator* of $\mathbf{F}_r$; that is, every nonzero element of $\mathbf{F}_r$ will be a power of C. If $s = (r-1)/n$, then the matrix $A = C^s$ is a principal nth root of unity. Hence, A is a root of $c_n(x)$ and the characteristic polynomial of A is an irreducible (over $\mathbf{F}_q$) factor of $c_n(x)$. The other irreducible factors of $c_n(x)$ are the characteristic polynomials of A^k for k relatively prime to n.

The second method makes use of the companion matrix A of the nth degree polynomial $p(x)$. If a nonzero vector $\mathbf{v}$ is found such that the set $\{\mathbf{v}, A\mathbf{v}, \ldots, A^k\mathbf{v}\}$ is dependent for some $k < n$, then the dependency coefficients $a_0, a_1, \ldots, a_k$ such that $a_0\mathbf{v} + a_1 A\mathbf{v} + \ldots + a_k A^k\mathbf{v} = \mathbf{0}$ define a polynomial $a(x) = a_0 + a_1x + \ldots + a_k x^k$ which has a nontrivial factor in common with $p(x)$. This factor can be easily obtained using the Euclidean algorithm for gcd $(p(x), a(x))$. The problem with this method is in locating a suitable vector $\mathbf{v}$. It is hoped that further investigation will solve this problem.

Multiresolution Morphological Image Coding

Researcher: Professor William Douglas Withers

Although, linear data transforms, such as the discrete cosine transform or various wavelet transforms, have enjoyed considerable popularity and success as tools for image processing and image coding, they lack power to succinctly express many common image features - particularly discontinuous features such as sharp edges. This project is investigating the development and use of new types of transforms specifically adapted to common image structures, with the goal of creating new image formats capable of expressing images both higher in quality images and smaller in data quantity than existing formats.

Research Course Projects

Global Modeling and Simulation Integration 2001 Supporting the MIW C4I Gateway

Researcher: Midshipman 1/C Patricia Leyland, USN
Adviser: Professor Thomas J. Sanders
Sponsor: Christopher Scannell, Advanced Information Technology Branch,
Naval Research Laboratory (NRL)

This project had two objectives.

1) Developing mine warfare scenarios for use in Global Modeling and Simulation Integration 2001.
   a) Helicopter sweeping a minefield.
   b) CG-47 encountering a minefield.

2) Providing on-site technical support at the Naval War College, which was the site for the Naval war games.
   a) MIW C4I Gateway trouble shooting.
   b) Testing software being developed for the exercise.
   c) Providing backup options when problems arose.

The sponsor's software was to serve as a bridge or a two-way connection between programs such as JSAF and GCCS-M. It was transported to the Naval War College for use in war games. The researcher was there during the crunch time of the operation and the implantation at the War College. The experience provided the researcher with opportunities to widen her knowledge of computers, to ask questions of a variety of high ranking officers about her future area of focus, to see how the military prepares for wars using computers and technology, and to see that many people work extremely hard to try to make our navy top rate.

JSAF and PCSWAT

Researchers: Midshipman 1/C Robert Niemeyer, USN
and Midshipman 1/C Alexander Goodno, USN
Adviser: Professor Thomas J. Sanders
Sponsor: Joseph Collins, Advanced Information Technology Branch,
Naval Research Laboratory (NRL)

The objective of this study was to test a new version of JSAF that was to be used in the Global 2001 simulation that took place at the Naval War College in Newport, RI. JSAF is a war-gamming simulator still in the developmental stages of use in the navy's war-gaming sector. The newer version was being used so that a wider array of environmental factors could be incorporated in the exercise. Our task was to compare collected data and JSAF outputs for the AQS-14 and AQS-20 sonar buoys on MH-53 minesweeping helos to try to determine if the JSAF model was adequate for the exercise.

The project was only partially completed. Although significant testing took place, computer resources were not adequate to complete the project. Among the results that were obtained was the identification of an error in the system that the programmers hoped to be able to rectify by the time Global 2001 began. No further work on the project is expected to be done by the researchers.

From 0's and 1's To Music In The Air: The Compact Disk

Researcher: Midshipman 1/C Philip Ely, USN
Adviser: Associate Professor JoAnn Turisco

This research project began with a reading course in the fall of 2001. He read the A First Course in Coding Theory, by Raymond Hill, and Applications of Abstract Algebra with Maple, by Richard Klima, Neil Sigmon, and Ernest Stitzinger. Most of fall semester was spent studying the mathematics necessary for an understanding of various codes such as linear codes, Hamming codes, and cyclic codes.

During the spring semester, the researcher concentrated more on BCH and Reed-Solomon codes and their applications to the compact disk. He presented his work both at the Service Academy conference in April and for members of the Honors Committee. His final paper contains the mathematical background utilized in coding theory and also includes Maple procedures for error correction in a Hamming and Reed-Solomon code.

The Application of Elliptic Curves to Public Key Cryptography

Researcher: Midshipman 1/C Richard Linnell, USN
Adviser: Associate Professor JoAnn Turisco

The researcher began his studies during the summer of 2001 by reading Rational Points On Elliptic Curves, by Joseph H. Silverman and John Tate. He continued studying elliptic curves in a reading course during the fall semester 2001.

During the spring semester, the reseacher concentrated more on his study of cryptography. He read Applications of Abstract Algebra with Maple, by Richard Klima, Neil Sigmon, and Ernest Stitzinger, and Elliptic Curves and their Applications Cryptography, by Andreas Enge. He presented his work both at the Service Academy Conference in April and for members of the Honors Committee. His paper contains a background of projective geometry, elliptic curves, cryptography, and examples, using Maple procedures, of elliptic curves over finite fields.

Trident Scholar Projects

Covert Communication Utilizing Discretely Generated Chaos

Researcher: Midshipman 1/C Noah F. Reddell, USN
Advisers: Associate Professor Erik M. Bollt
and Commander Thaddeus B. Welch, III, USN (Electrical Engineering Department)

Chaotic systems are aperiodic, deterministic, and sensitive to slight variations in initial condition. The latter property presents the problem that behavior of the system cannot be predicted for a significant period of time even though for the next instant, it is completely predictable.

The frequency domain and time domain properties of chaotic systems have generated interest in the military communications field. Midshipman Reddell explored the advantages of a communication system based on a chaotic carrier for military purposes. He used digital signal processing techniques to implement the system, perform frequency domain analysis, and generate system performance curves. A series of computer simulations were used to enhance system performance.

He developed a digital transmitter that is difficult to localize and detect by exploiting some of the natural properties of chaotic systems. The use of discrete methods allowed for considerable improvement over earlier schemes.

He demonstrated a new dual synchronizing receiver scheme that works by storing samples over an entire bit period prior to estimation. Results show significantly better bit error probability performance in comparison to previously published methods. He also developed a systematic method to further improve the bit error performance and covertness of the system by optimizing the selection of the modulation parameters. This involved a comparison of the average energy per bit and testing each parameter set for stability using the Lyapunov exponent method.

Research concentrated on developing a system that works effectively without a conspicuous signature in the frequency domain. Such a system could be extremely useful for covert wireless communications.

Modeling Morphogenesis with Reaction-Diffusion Equations Using Galerkin Spectral Methods

Researcher: Midshipman 1/C Benjamin M. Heineike, USN
Advisers: Professor Reza Malek-Madani and Associate Professor Sonia M. Garcia

This project studied the nonhomogeneous steady-state solutions of the Gray-Scott model, a system of nonlinear partial differential equations that has received attention in the past decade in the context of pattern formation and morphogenesis. Morphogenesis, or 'birth of shape', is the biological term for the initial formation of patterns that occur in development as cells begin to differentiate. The model is a two morphogen reaction-diffusion system in which individual molecules display complex self-organization in aggregate.

The project was divided into two main parts. The first part developed the Galerkin Spectral method for application to the two species reaction-diffusion system. Limitations and capabilities of the Galerkin Spectral method were discussed in the context of the heat equation, the Burgers equation, and the Allen-Cahn equation.

The second part analyzed the stability of equilibria in the Gray-Scott model in terms of reaction and diffusion parameters. A region of Hopf bifurcation is identified for the diffusionless system, and conditions for diffusion driven instability are developed. We showed, in particular, that diffusion driven instability occurs only when the diffusion constants of each morphogen are different in any two species reaction-diffusion equation. We then showed some numerical simulations of pattern formation in the Gray-Scott model using MATLAB programs to implement the Galerkin Spectral method.

Faculty Publications

Journal (Refereed) Manuscripts

Benkart, Georgia M., GAGLIONE, Anthony M., Professor, JOYNER, W. David, Professor, KIDWELL, Mark E., Professor, MEYERSON, Mark D., Professor, Spellman, Dennis, and WARDLAW, William P., Professor, "Principal Ideals and Associate Rings," *JP Journal of Algebra, Number Theory and Applications,* 2(2), pp.181-193 (2002).

A commutative ring A with 1 is **associate** provided whenever two elements a and b generate the same principal ideal there is a unit u such that ua = b. The main results of this paper are:

1. Every commutative Noetherian ring with 1 is a subdirect product of rings which have the property that all their unital subrings are associate.
2. Every commuataive ring embeds into an associate ring.
3. Every commutative unital algebraically closed or principal ring is associate.
4. The direct product of associate rings is associate.

One novel feature here is that we prove these results using model theory. For comparison and completeness, the main result is also sketched using a localization argument.

Billings, Laura, BOLLT, Erik M., Associate Professor, and Schwartz, I.B., "Phase-Space Transport of Stochastic Chaos in Population Dynamics of Virus Spread," *Physical Review Letters*, 88 (2002), article # 234101.

A general way to classify stochastic chaos is presented and applied to population dynamics models. A stochastic dynamical theory is used to develop an algorithmic tool to measure the transport across basin boundaries and predict the most probable regions of transport created by noise. The results of this tool are illustrated on a model of virus spread in a large population, where transport regions reveal how noise completes the necessary manifold intersections for the creation of emerging stochastic chaos.

BOLLT, Erik M., Associate Professor and Klebanoff, Aaron, "A New and Simple Chaos Toy," cover article: *International Journal of Bifurcation and Chaos*, 12(8), pp.1843 – 1857 (2002).

We present two new, and perhaps the simplest yet, mechanical chaos demonstrations. They are both designed based on a recipe of competing nonlinear oscillations. One of these devices is simple enough that using the provided description, it can be built using a bicycle wheel, a piece of wood routed with an elliptical track, and a ball bearing. We provide a thorough Lagrangian mechanics based derivation of equations of motion, and a proof of chaos based on showing existence of an embedded Smale horeshoe using Melnikov's method. We conclude with discussion of a future application.

BOLLT, Erik M., Associate Professor, "Review of Chaos Communication by Feedback Control of Symbolic Dynamics," *International Journal of Bifurcation and Chaos*, 13(2), pp.269-285, (2003).

This paper is meant to serve as a tutorial describing the link between symbolic dynamics as a description of a chaotic attractor, and how to use control of chaos to manipulate the corresponding symbolic dynamics to transmit an information-bearing signal. We use the Lorenz attractor, in the form of the discrete successive maxima map of the z-variable time-series, as our main example. For the first time, here, we use this oscillator as a chaotic signal carrier. We review the many previously developed issues necessary to create a working control of symbol dynamics system. These include a brief review of the theory of symbol dynamics, and how they arise from the flow of a differential equation. We also discuss the role of the (symbol dynamics) generating partition, the difficulty of finding such partitions, which is an open problem for most dynamical systems, and a newly developed algorithm to find the generating partition which relies just on knowing a large set of periodic orbits. We also discuss the importance of using a generating partition in terms of considering the possibility of using some other arbitrary partition, with discussion of consequences both generally to characterizing the system, and also specifically to communicating on chaotic signal carriers. Also, of practical importance, we review the necessary feedback-control issues to force the flow of a chaotic differential equation to carry a desired message.

BOLLT, Erik M., Associate Professor, "Combinatorial Control of Global Dynamics in a Chaotic Differential Equation," *International Journal of Bifurcation and Chaos*, 11(8) pp. 2145-2162, 2001.

Controlling chaos has been an extremely active area of research in applied dynamical systems, following the introduction of the Ott, Grebogi, Yorke (OGY) technique in 1990 [Ott et al., 1990], but most of this research based on parametric feedback control uses local techniques. Associated with a dynamical system which pushes forward initial conditions in time, transfer operators, including the Frobenius–Perron operator, are associated dynamical systems which push forward ensemble distributions of initial conditions. We have shown that such global representations of a discrete dynamical system are useful in controlling certain aspects of a chaotic dynamical system which could only be accessible through such a global representation. Such aspects include invariant measure targeting, as well as orbit targeting. In this paper, we develop techniques to show that our previously discrete time techniques are accessible also to a differential equation. We focus on the Duong oscillator as an example. We also show that a recent extension of our techniques by G´ora and Boyarsky [1999] can be further simplified and represented in a convenient and compact way by using a tensor product.

BOLLT, Erik M., Associate Professor, Stanford, T., Lai, Y. C., and Zyczkowski, K., "What Symbolic Dynamics Do We Get with a Misplaced Partition? On the Validity of Threshold Crossings Analysis of Chaotic Time-Series," *Physica D*, 154 (3-4), pp. 259-286, 2001.

An increasingly popular method of encoding chaotic time-series from physical experiments is the so-called threshold crossings technique, where one simply replaces the real valued data with symbolic data of relative positions to an arbitrary partition at discrete times. The implication has been that this symbolic encoding describes the original dynamical system. On the other hand, the literature on generating partitions of non-hyperbolic dynamical systems has shown that a good partition is non-trivial to find. It is believed that the generating partition of non-uniformly hyperbolic dynamical system connects "primary tangencies," which are generally not simple lines as used by threshold crossings. Therefore, we investigate consequences of using itineraries generated by a non-generating partition. We do most of our rigorous analysis using the tent map as a benchmark example, but show numerically that our results likely generalize. In summary, we find the misrepresentation of the dynamical system by "sample-path" symbolic dynamics of an arbitrary partition can be severe, including (sometimes extremely) diminished topological entropy, and a high degree of non-uniqueness. Interestingly, we find topological entropy as a function of misplacement to be devil's staircase-like, but surprisingly non-monotone.

Davidchack, R. L., Lai, Y. C., Klebanoff, A., and BOLLT, Erik M., Associate Professor, "Towards Complete Detection of Unstable Periodic Orbits in Chaotic Systems," *Physics Letters A*, 287, pp. 99-104, 2001.

We present a rigorous analysis and numerical evidence indicating that a recently developed methodology for detecting unstable periodic orbits is capable of yielding *all* orbits up to periods limited only by the computer precision. In particular, we argue that an efficient convergence to every periodic orbit can be achieved and the basin of attraction can be made finite and accessible for typical or particularly chosen initial conditions.

Fourte, Michael, and JOYNER, W. David, Professor, "Odd King Tours on Even Chessboards," *Journal of Recreational Mathematics*, Vol. 31, pp. 173-177 (2003).

In this paper we show that there is no complete odd king tour on an even chessboard, partially answering a question raised by Bailey and Kidwell.

GAGLIONE, Anthony M., Professor, (co-author), "Basic Commutators as Relators I," *Journal of Group Theory*, 5, pp. 351-363 (2002).

Charles Sims has asked whether or not the lower central subgroup $\gamma_n(F)$ of a free group F coincides with the normal closure in F of the set of basic commutators of weight n. In part I, we investigate variations of this question where we consider other varieties or other sets of commutators. We also give brief new proofs that the question has a positive answer in the previously known cases for weight n at most 4 and for the case where n = 5 and F is free with rank 2. In part II, we will show that Sims' question has a positive answer for the case where n = 5 and F is free with rank 3. In part III, we will use the results of the first two parts to show that Sims question always has a positive answer for weight 5.

GAGLIONE, Anthony M., Professor, (co-author), "Groups Whose Universal Theory Is Axiomatizable by Quasi-identities," *Journal of Group Theory*, 5, pp. 365-381 (2002).

Discriminating groups were introduced by Baumslag, Myasnikov and Remeslennikov with an eye toward applications to the universal theory of various groups. In a previous paper of the authors it was shown that if G is any discriminating group then the universal theory of G coincided with that of its direct square GxG. In this paper, we explore groups G whose universal theory coincides with that of their direct square. These are called squarelike groups. We show among other things that the class of squarelike groups is first-order axiomatizable and contains the class of discriminating groups as a proper subclass. Further we show that the class of discriminating groups is not first-order axiomatizable.

GAGLIONE, Anthony M., Professor, (co-author), "Every Abelian Group Universally Equivalent to a Discriminating Group is Elementarily Equivalent to a Discriminating Group," Combinatorial and Geometric Group Theory, Clary, et. al. (eds), *Contemporary Math*, 296, pp.129-137 (2002).

Some open questions were posed in the above paper. Among them were the following two:

a. Is every squarelike group the direct union of a family of discriminating groups?
b. Is every squarlike group elementarily equivalent to a discriminating group?

Here we answer question (a) affirmatively for the special case of torsion abelian groups. We also answer (b) affirmatively for the class of all abelian groups.

HERRMANN, Robert A., Professor, "Hyperfinite and Standard Unifications for Physical Theories," *International Journal of Mathematics and Mathematical Sciences*, 28(2) 93-102, 2001.

Let a set of physical theories be represented by a nonempty subset $\{S^{V}_{N(j)} \mid j \in N\}$ of the lattice of consequence operators defined on a language . It is established that there exists a unifying injection defined on the nonempty set of significant representations for natural-systems $M \subset \Lambda$. If $W \in M$, then Σ_W is a hyperfinite ultralogic and $\cup\{\mathbf{S}^{\mathbf{V}}_{\mathbf{N}(j)}(\mathbf{W}) \mid j \in N\} = \Sigma_W(*\mathbf{W}) \cap \Lambda$. A product hyperfinite ultralogic Π is defined on internal subsets of $*\Lambda^{m}$ and shown to represent the application of Σ to $\{W_1, \ldots, W_m\} \subset M$. There also exists a standard unifying injection S_W such that $\Sigma_W(*\mathbf{W}) \subset \mathbf{S_W}(*\mathbf{W})$.

HERRMANN, Robert A., Professor, "Ultralogics and Probability Models," *International Journal of Mathematics and Mathematical Sciences*, 27(5), pp. 321-325, 2001.

In this paper, we show how nonstandard consequence operators, ultralogics, can generate the general informational content displayed by probability models. In particular, a probability model that predicts that a specific single event will occur and those models that predict that a specific distribution of events will occur.

HERRMANN, Robert A., Professor, "The Non-random Character and Intelligent Design of 'Chance' Events," *TJ*, 15(2), pp. 103-109, 2001.

Recent advances in general design theory are discussed. In particular, a signature that implies that "randomness" is, in general, intelligently designed and that all natural-system behavior that is deemed as probabilistic in character is specifically designed, produced, coordinated and sustained by a higher intelligence, by ultralogics. These conclusions are based upon an interpretation for mathematically obtained results and indirect evidence.

HOFFMAN, Michael E., Professor, "An Analog of Covering Space Theory for Ranked Posets," *Electronic Journal of Combinatorics*, 8(1) Research Paper 32, 12 pp., 2001.

Suppose *P* is a partially ordered set that is locally finite, has a least element, and admits a rank function. We call *P* a weighted-relation poset if all the covering relations of *P* are assigned a positive integer weight. We develop a theory of covering maps for weighted-relation posets, and in particular show that any weighted-relation poset *P* has a universal cover unique up to isomorphism.

JOYNER, W. David, Professor, '"Arithmetic of Characters of Generalized Symmetric Groups," *Archiv der Mathematik*, in press.

The result here answers the following questions in the affirmative: Can the Galois action on all abelian (Galois) fieldsK/Q be realized explicitly via an action on characters of some finite group? Are all subfields of a cyclotomic field of the form Q(c), for some irreducible character c of a finite group G? In particular, we explicitly determine

the Galois action on all irreducible characters of the generalized symmetric groups. We also determine the "smallest" extension of Q required to realize (using matrices) a given irreducible representation of a generalized symmetric group.

LOCKHART, Jody M., Associate Professor, and WARDLAW, William P., Professor, Problem 1638, Mathematics Magazine, Vol. 75, No. 1, 63, February 2002.

Let m be a positive integer. Show that there are infinitely many positive integers k such that m is a divisor of f_k and $f_{k+1} - 1$, where f_n denotes the n-th Fibonacci number.

LOCKHART, Robert B., Associate Professor, and Steiner, Michael, "Preserving Entanglement Under Perturbation and Sandwiching All Separable States," *Physical Review A*, 65, # 022107.

In this paper, the researchers created open neighborhoods consisting solely of entangled states for many entangled pure states. Among those included are all maximally entangled states and all bipartite pure entangled states. One of the consequences of the existence of these neighborhoods is the creation of a sandwich inside of which all separable states must lie. As dimension goes up, this sandwich shrinks in width.

LOCKHART, Robert B., Associate Professor, "Low-rank Separable States Are a Set of Measure Zero Within the Set of Low-rank States," *Physical Review A*, June 2002.

In this paper, the author used Sard's theorem to show that the set of low-rank separable states are a set of measure zero within the set of low rank states. The proof is relies on characterizing the ranges of separable operators and relating them to Grassmannians.

LOCKHART, Robert B., Associate Professor, and Steiner, Michael J., and Gerlach, Karl, "The Geometry of Product States," *Quantum Information and Computation*, Vol. 2, No. 5, pp. 333-347 (2002).

In this paper, we analyze various properties of properties of product states. For instance, we show that in the bipartite case the closest product state to a maximally entangled state is the totally mixed state. We also show that all states in the space tangent to the manifold of product states at the totally mixed state are separable.

McCOY, Peter A., Professor, "On Radiating Solutions to the Helmholtz Equation," *Applicable Analysis*, Vol. 77, nos. 3-4, pp. 319-325, (communicated by Yongzhi Xu), 2001.

This paper uses far field patterns to develop information about the singularities of solutions of the Helmholtz equation.

MICHAEL, T. S., Associate Professor, "Signed Degree Sequences and Multigraphs," *Journal of Graph Theory*, Vol. 41, pp. 101-105 (2002).

We give necessary and sufficient conditions for a sequence of integers to be the signed degree sequence of a signed multigraph. Our main theorem completely solves a problem in the recent literature of graph theory.

MICHAEL, T. S., Associate Professor and Quint, Thomas, "Sphere of Influence Graphs and the L-Infinity Metric," *Discrete Applied Mathematics*, accepted for publication.

We introduce sphere of influence graphs (SIGs) in the L-infinity metric and study their fundamental properties. We argue that SIGs defined with the L-infinity metric are superior to the Euclidean SIGs of Toussaint in capturing

low-level perceptual information in certain dot patterns. Every graph without isolated vertices is a SIG in the L-infinity metric for all sufficiently high dimensions, and this allows us to define a graphical parameter, the SIG-dimension, that is akin to boxicity. We determine the SIG-dimensions for some classes of graphs and obtain inequalities for others.

MICHAEL, T.S., Associate Professor, and TRAVES, William N., Assistant Professor, "The Roller-Coaster Conjecture and Independence Sequences of Well-Covered Graphs," *Graphs and Combinatorics*, accepted for publication.

A graph G is well-covered provided each maximal independent set of vertices has the same cardinality. The term s_k of the independence sequence $(s_0,s_1,...,s_á)$ equals the number of independent k-sets of vertices of G. We investigate constraints on the linear orderings of the terms of the independence sequence of well-covered graphs. In particular, we provide a counterexample to the recent unimodality conjecture of Brown, Dilcher, and Nowakowski. We formulate the Roller-Coaster Conjecture to describe the possible orderings among the terms of the independence sequence.

Pinzon, J. E., PIERCE, John F., Associate Professor, Tucker, C. J., and Brown, M., "Evaluating Coherence of Natural Images by Smoothness Membership in Besov Spaces," *Institute for Electrical and Electronic Engineering (IEEE) Transactions on Geoscience and Remote Sensing*, Vol. 39, pp. 1879-1889, September 2001.

Smoothness membership in Besov Spaces B^{∞}_{q} (*I*) is used to compare the spatial coherence of satellite images. Smoothness is given by a complexity index computed as the rate of decay of the approximation error, $\varepsilon(M)$, when the image is approximated by its *M* largest quantized wavelet coefficients. The technique was applied to a set of nine Normalized Difference Vegetation Index (NDVI) time series data as a quantitative quality measure of spatial coherence. The NDVI data set comprises different composite and atmospheric correction techniques. The estimates of the complexity index give a quantitative measure of the performance of these techniques that agrees well with visual evaluation and with the physics of the image collection process. We demonstrate that the maximum value NDVI composes with Rayleigh, ozone, and water vapor correction to consistently provide the highest spatial coherence among the composites and atmospheric correction techniques evaluated. We also show the complexity index is regionally dependent and is higher in dry periods than in wet periods, where residual cloud interference is more likely to appear.

PRICE, Geoffrey L., Professor, and Arveson, W. B., "Infinite Tensor Products of Completely Positive Semigroups," *Journal of Evolution Equations*, Vol. 1, pp. 221-242 (2001).

Since virtually the beginning of the study of quantum mechanics physicists have used operator algebras as models to understand the behavior of quantum mechanical systems. In this setting the elements of an operator algebra *A* are viewed as the physical observables, and there is a one-parameter group of automorphisms $\{\alpha_t : t \geq 0\}$ defined on *A* so that for each observable x the operator $\alpha_t(x)$ represents the evolution of x at time t. Physicists say that the system "returns to equilibrium" if there is a normal state ω on *A* such that for any other normal state ρ on *A*, the states $\rho o \alpha_t$ approach for large t. Such a state is said to be absorbing. Recently R. T. Powers has studied quantum dynamical systems called E_0-semigroups. These are similar to the one-parameter groups of automorphisms above but they may not move backward in time. An important question in the subject is to determine if there are E_0-semigroups that have no absorbing states. Powers showed that for a large class of these semigroups each E_0-semigroup in the class is equivalent to one with an absorbing state. In this paper the authors have shown that there are examples of E_0-semigroups that are pure (i.e., there are no nontrivial subalgebras of *A* left globally invariant) but which have no absorbing states. On the other hand, by Powers' result such E_0-semigroups are equivalent to pure E_0-semigroups that do have an absorbing state.

Qingxian Xie, Guanrong Chen, and BOLLT, Erik M., Associate Professor, "Hybrid Chaos Synchronization and Its Application in Information Processing," *Math Comput Modeling* 35, pp.145-163, 2002.

In this paper, through numerical studies, we explore a new methodology for chaos syn-chronization via a hybrid (generalized plus identical) synchronization. An arbitrary signal, generated by an unknown dynamical system, can be synchronized by the hybrid chaotic system. The signal can then be stored for future application such as password and message identification. Each finite-length signal can, in principle, be labeled and stored by a unique number, provided that the key hybrid system parameter used for the purpose is suitably chosen within a one-to-one mapping range. The new methodology enables us to encode an arbitrary signal accurately and efficiently. Sufficient numerical simulations are shown to verify the proposed design. Potential applications of the developed hybrid chaos synchronization system include information storage, message identification, and certain types of secure signal and image communication.

Saito, Mutsumi and TRAVES, William N., Assistant Professor, "Differential Algebras on Semigroup Algebas," *Contemporary Mathematics*, Vol. 286, pp. 207-226, December 2001.

This paper studies algebra of operators associated to a semigroup algebra. The ring of differential operators is shown to be anti-isomorphic to the symmetry algebra and both are described explicitly in terms of the semigroup. As an application, we produce a criterion to determine the equivalence of A-hypergeometric systems. Conditions under which associated algebras are finitely generated are studied. The results are sufficient to establish Becker's conjecture in the semigroup case. As well, an algorithm is provided to compute the composition series of D-modules over semigroup algebras.

TRAVES, William N., Assistant Professor, "Localization of the Hasse-Schmidt Algebra," *Canadian Math Bulletin*, Vol. 46, no. 2, pp. 304-309, 2002.

The behaviour of the Hasse-Schmidt algebra of higher derivations under localization is studied using Andre cohomology. Elementary techniques are used to describe the Hasse-Schmidt derivations on certain monomial rings in the nonmodular case. The localization conjecture is then verified for all monomial rings.

WARDLAW, William P., Professor, and WITHERS, William D., Professor, Problem 10888, *American Mathematical Monthly*, Vol. 108, No. 7, 667, August-September 2001.

A groupoid is a set together with a binary operation. A groupoid with a binary operation $*$ is a quasigroup if whenever any two of x, y, and z are given, the equation $x*y = z$ uniquely determines the third. If $(S, *)$ and $(T, \circ)$ are groupoids, then a mapping $\phi: S \to T$ satisfying $\phi(x*y) = \phi(x)\circ\phi(y)$ is a homomorphism. Prove or disprove: Every homomorphic image of a quasigroup is a quasigroup.

WARDLAW, William P., Professor, "A Generalized General Associative Law," *Mathematics Magazine,* Vol. 74, No. 3, 230-233, June 2001.

This paper first reviews various proofs of the generalized associative law in the literature and points out the shortcomings and fallacies in some of them. Then it is recommended that the general associative law be replaced with a generalization, namely that n-associativity implies $(n + 1)$-associativity when $n > 2$.

WARDLAW, William P., Professor, Solution 1608, *Mathematics Magazine*, Vol. 74, No. 5, 404, December 2001.

Proposed by William D. Weakly, Indiana-Purdue University at Fort Wayne, Fort Wayne, IN. Let b be a positive integer, $b > 1$. We call a positive integer onederful in the base b if it divides some integer whose base b representation is all ones. Which positive integers are onederful in the base b?

Solution by William P. Wardlaw, U.S. Naval Academy, Annapolis, MD.

A positive integer n is onederful in the base b if and only if n is relatively prime to b. First observe that if n divides $(111\ldots11)_b = 1 + b + b^2 + \ldots + b^r$ for some r, then clearly n is relatively prime to b. Conversely, if n is relatively prime to b, then $m = (b - 1)n$ is also relatively prime to b. Hence, by the Euler-Fermat theorem, m divides $b^{\phi(m)} - 1$. It follows that n divides $(b^{\phi(m)} - 1)/(b - 1) = b^{\phi(m)} + \ldots + b^2 + b + 1 = (11\ldots111)_b$.

WITHERS, William Douglas, Professor, "A Rapid Probability Estimator and Binary Arithmetic Coder", *Institute for Electrical and Electronic Engineering (IEEE) Transactions on Information Theory*, 47-4, pp. 1533-1537, 2001.

We present a new integrated algorithm for binary arithmetic coding and probability estimation, competitive in speed and compression performance with state-of-the-art algorithms such as the QM-coder and Z-coder. The chief innovation is representing the bracketing interval width both directly and by a logarithmic approximation. Performance is evaluated by experiments using bilevel-image data sets. An open-source software version is available.

Conference Proceedings

BUCHANAN J., Professor, Cristini P., Gilbert R., Wirgin A. and Xu Y., "A Mode-matching Method for Forward and Inverse Scattering from an Object in a Shallow-water Waveguide," *Theoretical and Computational Acoustics '99, Actes du colloque: 4th Intl. Conf. Theoret. Computat. Acoustics*, Trieste, 10-14 May 1999.

BUCHANAN J., Professor, Gilbert R.,Wirgin A. and Xu Y., "Unambiguous Reconstruction of the 2D Boundary of a Half-space Probed by Acoustic Waves," *Proceedings of 3rd International ISAAC Congress, Actes du colloque: 3rd International ISAAC Congress*, Berlin, 2025 August 2001.

HOFFMAN, Michael E., Professor, "Periods of Mirrors and Multiple Zeta Values," *Proceedings of the American Mathematical Society*, Vol. 130, pp. 971-974, 2002.

In a recent paper, A. Ligober showed that the multiplicative sequence $\{Q_i(c_1,\ldots,c_i)\}$ associated to the power series $Q(z)=\Gamma(1+z)^{-1}$ appears in a relation between the Chern classes of certain Calabi-Yau manifolds and the periods of their mirrors. We show that the polynomials Q_i can be expressed in terms of multiple zeta values.

KONKOWSKI, Deborah A., Professor, "Quantum Singularity of Quasiregular Spacetimes," *Proceedings of the 9th Marcel Grossmann Meeting on General Relativity*, (ed. V.G. Gurzadyan), R.T. Jantzen, and R. Ruffini, Singapore: World Scientific, 987, 2002.

A class of spacetimes with classical quasiregular singularities is shown to be quantum mechanically singular as well. These static spacetimes with dislocations and disclinations are quantum-mechanically singular since the spatial portion of the wave operator is not essentially self-adjoint and thus the evolution of a test quantum wave packet is not uniquely determined by the initial wave function.

KONKOWSKI, Deborah A., Professor, "Quantum Singularity of Spacetimes with Dislocations and Disclinations," *Proceedings of the 20th Texas Symposium on Relativistic Astrophysics*, pp. 879-881, 2002.

Spacetimes with dislocations and disclincations are classically singular. The authors show that they are quantum mechanically singular as well using a definition first proposed by Horowitz and Marolf in 1995.

LIAKOS, Anastasios P., Assistant Professor, Swannack, C. H., Cox, C. L., and Hirt, D. E., "Nanocomposite Modeling and Simulation," *Proceedings of SPE ANTEC*, San Francisco, May 2002. Appears in: http://www.4spe.org/bookstore/books/antec2002index.pdf

Nanocomposite polymer films are known to exhibit increased barrier properties at low additive loadings. These films, particularly at low loadings, are of interest to the food packaging industry. However, current 2D models do not fully account for the characteristics of typical polymer-clay systems. The results of a new permeation simulation using Monte Carlo techniques will be presented.

Optimized Monte Carlo simulations were run in three dimensions to determine the effective diffusivity coefficients for typical polymer clay systems. Systems with loadings between 0.5% and 50% were simulated. The results were compared to existing models to examine the effects the added dimension has on the diffusion coefficient. The results when then viewed using Java3D to examine the validity and analyze the process.

Miller, David O., Schwemmer, Geary K., and GARCIA, Sonia M. F., Associate Professor, "Preliminary Measurements of Aerosol Backscatter/extinction Ratios Using HARLIE During HARGLO-*2," Proceedings of the 21st International Laser Radar Conference*, pp. 595-597, 2002.

Aerosol backscatter lidar provides both high temporal and special resolution measurements of the aerosol structure of the atmosphere. Knowledge of the optical and physical properties of the aerosols is necessary in order to calculate aerosol backscatter and extinction unless the lidar observations are supplemented with an external calibration, such as the aerosol optical depth of the layer (Fernald, et. al). Data collected during the HARGLO-2 wind intercomparison at the NASA Wallops Flight Facility are calibrated using aerosol optical depth measurements from an Aerosol Robotic Network (AERONET) sun-photometer.

MICHAEL, T. S., Associate Professor, and Pinciu, Val, "Multiply Guarded Guards in Orthogonal Galleries," *Proceedings of the International Conference of Computing and Information (ICCI)*, San Francisco, Lecture Notes in Computer Science, Vol. 2073, pp. 753-762, Springer 2001.

Let P be a rectilinear polygon (the art gallery) with n sides. We wish to select a set G of points (the guards) so that (a) every point in the polygon is visible to some guard; and (b) every guard is visible to at least k other guards. What is the minimum number of guards g(n,k) that is guaranteed to suffice for all polygons with n sides? We prove that g(n,k) = (k+1)floor(n/6) + d, where d=1 if n is 2 less than a multiple of 6, and d=0 otherwise.

NAKOS, George C., Professor and Robert M. Williams: "Methods for the Object-Image Equations of N Points," *Proceedings of the 8th International Conference on Applications of Computer Algebra*, Volos, Greece, pp. 72-82, June 2002.

We assume that a set of three-dimensional points produces a two-dimensional image. Our goal is to describe relations between the coordinates of the object points and the image points without using the parameters of the transformation that has produced this image. These are known as object-image equations. Both the object points and the image points are determined up to a projective colineation. We base our approach on earlier work by Quan. Stiller, Asmuth, and Wan have produced a different set of object-image equations.

Book

JOYNER, W. David, Professor, "Rubik's Cube, Merlin's Machine, and Other Adventures with Groups," The Johns Hopkins University Press, May 2002.

In this book, we develop the basics of group theory and create group-theoretical models of Rubik's Cube-like puzzles. On the practical side, we also discuss the solution strategy for the Rubik's Cube in some detail. Some solution strategies are briefly discussed for similar puzzles (the '15 Puzzle', the 'Rubik tetrahedron' or Pyraminx, the 'Rubik dodecahedron' or Megaminx, the Skewb, the 'Hockeypuck', and the 'Masterball') as well. Because of our Rubik's Cube focus, the approach in this book is different from some texts:

a. there are a lot of non-standard, though relatively elementary, group theory topics;
b. we emphasize permutation groups via examples over general theory (such as Sylow theory);
c. we present some of the basic notions algorithmically; and
d. we include material which is interesting, from both the mathematical and puzzlists perspective, while keeping the level as low as possible for as long as possible.

Encyclopaedia of Mathematics

McCOY, Peter A., Professor, "Zonal Harmonics," Kluwer Encyclopaedia of Mathematics, Supplemental Volume III, Prof. M. Hazewinkel, managing editor, pp. 464-465, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2002.

This section of the Kluwer Math Encyclopedia gives the definition and a brief description of Zonal Harmonics. The description includes important properties and some applications on Zonal Harmonics to boundary-value problems associated with the axially symmetric Laplace's equation.

McCOY, Peter A., Professor, Signed Book Review for the American Mathematical Reviews (AMS 1-827-998), "Wavelets, Tools for Science and Technology," Stephane Jaffard, Yves Meyer and Robert D. Ryan, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, 2001.

This review is of the revised and up-dated book published by the author's in 1993. (See AMS MR95: 94005). Several sections of the revision have been expanded and include applications of contemporary interest in science and communication theory.

McCOY, Peter A., Professor, Signed Book Review for the Zentralblatt fur Mathematik (ZBL 01512760), "Plane-Wave Theory of Time-Domain Fields, Near-Field Scanning Applications," Thorkild B. Hansen and Arthur D. Yaghijan, Institute for Electrical and Electronic Engineering (IEEE) Press, New York, 2001.

This review describes an excellent advanced graduate or post doctorate level book in the IEEE Press Series on Electromagnetic Wave Theory. As the title describes, the subject is on Plane Wave Theory in the time domain and pays particular attention to Near-Field Scanning Applications.

Presentations

BAILEY, Craig K., Professor, "Distance on an Elliptical Earth," Maryland-District of Columbia-Virginia Section Meeting of the Mathematical Association of America (MAA), Blacksburg, VA, 19-20 October 2001.

BAKER, B. Mitchell, Professor, "Maximizing Subsystem Entropy for Two Qubit Systems," University of Maryland, Baltimore County (UMBC), Baltimore, MD, July 2001.

BOLLT, Erik M., Associate Professor, "How Hot is Hot? Modeling, Measurement and the Role of Partition Placement," Institut des Sciences Mathematiques (ISM) 2001, Montreal, Canada, 10-12 May 2002. (Plenary speaker)

BOLLT, Erik M., Associate Professor, "Analogies Between Computer Viruses, Biological Viruses, and Their Associated Immune Systems Special Focus" on "Mathematical Models and Methods in Epidemiology," Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) at Rutgers U., 10-14 June 2002. (Plenary speaker and Invited speaker)

BOLLT, Erik M., Associate Professor, "The Mathematical Modeling in Biology Workshop," Duke University, 2-3 May 2002. (Plenary speaker)

BOLLT, Erik M., Associate Professor, "Transport and Global Control in Deterministic and Stochastic Dynamical Systems," Duke University, January 2002. (Plenary speaker at colloquium)

BOLLT, Erik M., Associate Professor, "Transport and Global Control in Deterministic and Stochastic Dynamical Systems," William and Mary University, January 2002. (Plenary speaker at colloquium)

BOLLT, Erik M., Associate Professor, Center for Nonlinear and Complex Systems seminar, "Density Transport and Control: Applications of the Frobenius-Perron Operator in Deterministic and Stochastic Dynamical Systems," Duke University, 22 October 2001. (Plenary speaker)

BOLLT, Erik M., Associate Professor, **"**Reconstruction of Evolving, Non-Convex Curves from a Sequence of Single-Angle Projections," Society for Industrial and Applied Mathematics (SIAM): Imaging Science 2001, Boston, MA, 22 September 2001. (Plenary speaker)

BOLLT, Erik Matthew, Associate Professor, "Transport and Global Control: Applications of the Frobenius-Perron Operator in Deterministic and Stochastic Dynamical Systems," Clarkson University, January 2002. (Plenary speaker at colloquium)

CRAWFORD, Carol G., Professor and MEYERSON, MARK D., Professor, "Calculus Web Labs," Sectional Meeting of the Mathematical Association of America (MAA), St. Mary's College, MD, 13 April 2002.

GAGLIONE, Anthony M., Professor, "Every Abelian Group Universally Equivalent to a Discriminating Group is Elementarily Equivalent to a Discriminating Group," Groups St. Andrews in Oxford, UK, August 2001.

GAGLIONE, Anthony M., Professor, "Discriminating and Squarelike Groups," Albany Group Theory Conference, Albany, NY, 11-14 Oct. 2001.

GAGLIONE, Anthony M., Professor, "A Survey of Discriminating and Squarelike Groups, I" Special Session of the American Mathematical Society (AMS), Montreal, Canada, 3-5 May 2002.

GAGLIONE, Anthony M., Professor, "Taking Matters to their Logical Conclusion. Going to the Ultralimit!" Ohio-Denison Group Theory Conference, Dennison, OH, 17-19 May 2002.

GAGLIONE, Anthony M., Professor "Applications of Groups and Number Theory," Fairfield University, Fairfield CT, 12-13 November 2001.

GAGLIONE, Anthony M., Professor, "Discriminating and Squarelike Groups," U.S. Naval Academy Mathematics Department Colloquium, Annapolis, MD, February 2002.

GAGLIONE, Anthony M., Professor, "On Discriminating and Squarelike Groups," Temple University Seminar, 17-16 Feb. 2002.

HOFFMAN, Michael E., Professor, "Pruning Kreimer's Trees," Special Session on Combinatorial Hopf Algebras, Eastern Sectional Meeting of the American Mathematical Society (AMS), Montréal, Canada, 4 May 2002.

HOFFMAN, Michael E., Professor, "Covering Spaces for Posets," U.S. Naval Academy Mathematics Department Colloquium, Annapolis, MD, 12 September 2001.

HOFFMAN, Michael E., Professor, "Multiple Zeta Values: Applications and Theory," The Johns Hopkins University, Baltimore, MD, 5 November 2001.

HOFFMAN, Michael E., Professor, "Pruning Kreimer's Trees," U.S. Naval Academy Mathematics Department Colloquium, Annapolis, MD, 16 January 2002.

KONKOWSKI, Deborah A., Professor, "Extending the Definition of Quantum Singularity to Maxwell and Dirac Field Operators," The 16th International Conference on General Relativity and Gravitation, Durban, South Africa, 15-21 July 2001.

KONKOWSKI, Deborah A., Professor, "Status of Two Instability Conjectures," The 16th International Conference on General Relativity and Gravitation, Durban, South Africa, 15-21 July 2001.

KONKOWSKI, Deborah A., Professor, "Quantum Singularity of Quasiregular Spacetimes," The 16th International Conference on General Relativity and Gravitation, Durban, South Africa, 15-21 July 2001.

KONKOWSKI, Deborah A., Professor, "Extending the Definition of Quantum Singularity to Maxwell and Dirac Field Operators," 11th Midwest Gravity Meeting, University of Waterloo, Waterloo, Ontario, Canada, Oct. 2001.

KONKOWSKI, Deborah A., Professor, "Quantum Singularity as Indicated by Klein-Gordon, Maxwell, and Dirac Fields in Quasiregular Spacetimes," American Physical Society Meeting, Albuquerque, New Mexico, 20-23 April 2002.

KONKOWSKI, Deborah A., Professor, "Definition and Classification of Singularities in GR: Classical and Quantum," British Gravitational Symposium 2002, London, England, 10-11 June 2002.

KONKOWSKI, Deborah A., Professor, "Are Classically Singular Spacetimes Quantum Mechanically Singular As Well?" London Relativity Seminar, Queen Mary, University of London, London, UK, 29 May 2002.

LIAKOS, Anastasios P., Assistant Professor, "Diffusion in Nanocomposite Materials," Clemson University, Clemson, SC, 11-14 May 2002.

MAHAR, Thomas J., Associate Professor, "The Ghost Fluid Method and Godunov's Method for the Euler Equations of Fluid Flow," U.S. Naval Academy – Indian Head Laboratory Programs Review, Annapolis, MD, 2002.

MARUSZEWSKI, Richard F., Professor, "One Way Functions," U.S. Naval Academy Mathematics Department Colloquium, Annapolis, MD, Fall 2001.

McCOY, Peter A., Professor, "Problems in Electromagnetics of Interest to the Navy," Minisymposium on Grand Challenges Electromagnetics," Society for Industrial and Applied Mathematics (SIAM) Annual Meeting, San Diego, CA, 9 July 2001.

McCOY, Peter A., Professor, "Field Singularities and Source Location," Session on Inverse Problems and Remote Sensing, Society for Industrial and Applied Mathematics (SIAM) Annual Meeting, San Diego, CA, 10 July 2001.

McCOY, Peter A., Professor, "On the Structure of Electromagnetic Fields," Office of Naval Research (ONR) Workshop and Review, Annapolis, MD, 7 March 2002.

MELLES, Caroline G., Associate Professor, "Integral Closures of Ideals and Resolution of Singularities," U.S. Naval Academy Mathematics Department Colloquium, Annapolis, MD, 20 March 2002.

PENN, Howard L., Professor, "Home Run Hitting," Joint Mathematics Meeting, San Diego, CA, January 2002.

POPOVICI, Irina, Assistant Professor, "Boundaries in Complex Dynamical Systems," American University, Washington, D.C., November 2001.

PRICE, Geoffrey L., Professor, "The Combinatorics of Spin Systems," University of Delaware, Newark, DE, November 2001.

SANDERS, Thomas J., Professor, "Joint SAF and Midshipmen Academics," Navy Modeling and Simulation Management Office (NAVMSMO) Technical Interchange Meeting, Washington, DC, August 2001.

TRAVES, William N., Assistant Professor, "The Elliptic Curve Attack on RSA Encryption," Mathematical Association of America (MAA) Section Meeting, Blacksburg, VA, October 2002.

TRAVES, William N., Assistant Professor, "Differential Simplicity," Route 81 Conference, State University of New York (SUNY), Albany, NY, November 2002.

TRAVES, William N., Assistant Professor, "Algebraic Curves for Fun and Profit," Colloquium at American University, Washington, D.C., November 2002.

TRAVES, William N., Assistant Professor, "Parallel Computation of Grobner Bases," Commutative Algebra Special Session, American Mathematical Society (AMS) National Meeting, San Diego, CA, January 2002.

TRAVES, William N., Assistant Professor, "A Power Series Problem Motivated by the Localization Conjecture," Commutative Algebra Special Session, American Mathematical Society (AMS) Section Meeting, Ann Arbor, MI, March 2002.

TRAVES, William N., Assistant Professor, "Artin Level Algebras and the Roller-Coaster Conjecture," Conference on Zero-dimensional Schemes, Sicily, Italy, June 2002.

TRAVES, William N., Assistant Professor, "Applications of Grobner Bases," Maui High Performance Computing Center, Maui, HI, June 2002. (Invited lecture)

TRAVES, William N., Assistant Professor, "The Value of Money," U.S. Naval Academy, Summer Seminar Series, Annapolis, MD, June 2001.

TRAVES, William N., Assistant Professor, "Commutative Algebra and Network Reliability," National Security Agency, June 2001. (Invited lecture)

TRAVES, William N., Assistant Professor, "Commutative Algebra and Network Reliability," Communications Security Enterprise (Canadian Version of National Security Agency), July 2001. (Invited lecture)

TRAVES, William N., Assistant Professor, "Introduction to Commutative Algebra and Simplicial Complexes," George Washington University Algebra Seminar, Fall 2002. [3 lectures]

TURNER, John C., Professor, "A Spreadsheet for Fisher's Exact Test," Joint Meeting of the American Statistical Association, Atlanta, GA, August 2001.

WARDLAW, William P., Professor, "Factoring Polynomials with Matrices, I," Fall Meeting of the Maryland-Virginia-District of Columbia Section of the Mathematical Association of America (MAA), Blacksburg, VA, 20 October 2001.

WARDLAW, William P., Professor, "Factoring Polynomials with Matrices, II," Spring meeting of the Maryland-Virginia-District of Columbia Section of the Mathematical Association of America (MAA), St. Mary's College, St. Mary's City, MD, 13 April 2002.

WITHERS, William Douglas, Professor, "Overview of JPEG 2000," U. S. Naval Academy Pure Mathematics Seminar, Annapolis, MD, 19 September 2001.

WITHERS, William Douglas, Professor, "Tufte on Presenting Data and Information," U. S. Naval Academy Pure Mathematics Seminar, Annapolis, MD, 17 April 2002.