Mathematics Department

Professor Michael W. Chamberlain
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. 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 either as Honors Mathematics Majors or in specially created projects under the guidance of faculty members. Several faculty spent many hours serving as mentors and readers for capstone projects required of all midshipmen majors. Listed next are some of our mathematics majors, their projects, and their faculty mentors:

Gerald Paul Lorio: "Fibonacci Sequences and Changing Determining Probability" (Professor Mark E. Kidwell)

Scott Charles McKinney: "Wavelets and Approximation Theory" (Professor Peter R. Turner)

Evelyn Ann Melo: "Fractals, They're Everywhere!" (Professor W. D. Withers)

Myah Christi Monjure: "Communicating with Chaos: Controlling Chaos to Transmit Messages" (Associate Professor Erik M. Bollt)

Craig Matthew Trent: "The Jeep on a Graph Problem" (Associate Professor T.S. Michael)

Once again, the USNA 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:

The Johns Hopkins University/Applied Physics Lab
Office of Naval Research
Naval Research Laboratory
Naval Air Warfare Center
Naval Surface Warfare Center
Naval Academy Research Council
National Science Foundation
National Security Agency
Natural Sciences & Engineering
Council of Canada

During the past year, members of the USNA Mathematics Department presented the results of their scholarly activities at 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.

Sponsored Research

Communicating Through Controlling Chaos

RESEARCHER: Midshipman 1/C Myah Monjure
ADVISER: Assistant Professor Erik M. Bollt
SPONSOR: Alumni Fund, Funded by USNA Academic Dean and Provost through the Chaos Lab

This project addresses problems in controlling chaos and controlling symbol dynamics with small perturbations. Recent work has demonstrated the utilization of symbolic dynamics representation of controlled chaotic orbits for communications with chaotic signal generators. The evolution of trajectories of a chaotic dynamical system is equivalent to symbolic dynamics in an appropriate symbol space. The recent advent of controlling chaos using the OGY (Ott, Grebogi, and Yorke) technique and a variety of targeting algorithms, with physical applications, has demonstrated that chaos can be mastered, and inherent instabilities can be used as an advantage in allowing small deliberate perturbations to cause large signal variations. Coupling control of chaos through small perturbations with learning the grammar of the corresponding symbol dynamics means that the control perturbations are actually a coding scheme on the original dynamics. Midn Monjure has successfully mastered the skills of chaos theory and some control theory necessary to force a trajectory generated by the Lorenz equations to follow a message which can be read, "Beat Army!"

Shallow Ocean Acoustics

RESEARCHER: Professor James L. Buchanan
SPONSORS: National Science Foundation (NSF) and Naval Research Laboratory (NRL)

In order to realistically model sound transmission in a shallow ocean the acoustic properties of the seabed must be taken into account. The seabed has been modeled variously as a completely rigid slab, a dense fluid, or an elastic slab. A more realistic model needs to admit the porous nature of most surficial sediments. In a poroelastic sediment model the seabed is taken to consist of a viscoeleastic frame with an interstitial pore fluid. For the last five years the researcher and his collaborators have been investigating sound transmission in the ocean over a poroelastic seabed. Recent work has included computing acoustic pressure in the near fields over a one layer seabed using a modal solution combined with integrals along certain branch cuts, computing acoustic pressure in an ocean with depth-varying sound speed, computing pressure in the far field over multi-layer seabed using modal solution, and computing pressure in the far field using a numerical technique called parabolic approximation.

The solution of the problem described above is a component of the solution of an important practical problem in ocean acoustics, that of recognizing the shape and/or composition of an object in the water or lying on the seabed. The investigator and his collaborators made progress on the problem of recognizing the location and shape of an object floating in the ocean under the simple assumption that the seabed is perfectly reflecting. Our approach was to simulate the scattered acoustic field by solving systems of linear equations derived from integrals and the acoustic field over the surface of the scatterer. Two methods of reconstructing the shape of the scatterer, assumed to be a solid of revolution, are being investigated. The first one is the Intersecting Canonical Boundary Approximations (ICBA), which attempts to match the acoustic field locally to the field of a cylinder. This method works well unless the source/receiver is located at a near null of the acoustic field. Hence for this method to be successful the frequency of the source must be varied to avoid such nulls.

Another limitation is that its yields an estimate of the radius of the object only at depths where a source/receiver unit is located. A second approach that was tried was to recover the Fourier coefficient of the scatterer. This method uses perturbation expansions of the integrals used to calculate the forward field to obtain expressions for the scattered field as a function of the Fourier coefficients of the scatterer. This allows calculation of the field efficiently enough to be used in an inversion scheme. This method is promising for two reasons. First, it is capable of determining the source to obstacle distance as part of the inversion process. Many inversion techniques require this distance to be known a priori. Second, it is capable of finding the location and dimension of the object from relatively sparse source-receiver configurations.

Further, worked planned on this problem includes extension of the technique to shapes more general than solids of revolution and use of the more sophisticated models of the seabed described above.

Acoustic Work

RESEARCHERS: Associate Professor Sonia M.Garcia and Steve Finette (NRL)
SPONSOR: Naval Research Laboratory (NRL)

NRL acoustic Steve Finette's group is working on unclassified projects in the general area of acoustic wave propagation in ocean waveguides, and they have an interest in new algorithms associated with both single frequency and pulse propagation in 3-D spatially varying deterministic or random media. I have been investigating a pseudo-spectral method of pulse propagation that involves the solution of an integral equation via a Green's function approach. They are particularly interested in looking at the stability and accuracy of the method, and would like to investigate variations/generalizations of this numerical approach for one-way (forward) propagation, analogous to one-way parabolic equation methods that they are currently using.

Closed-loop Degaussing Using Both Naval Vessels and Scale Physical Models

RESEARCHER: Associate Professor Gary O. Fowler
SPONSOR: Naval Surface Warfare Center (NSWC)

Naval vessels containing ferrous material emit detectable magnetic signals. NSWC administers a project that studies and measures this phenomenon. Data is collected from naval vessels under a variety of conditions and from scale models under similar conditions. A goal of the project is to connect these data in a manner that will allow measurements from the scale model to predict measurements on the naval vessel. This analysis is both statistical and mathematical in nature. It includes both the design of the experiments and the analysis of the data.

Stability of Spacetimes with Mild Singularities or Cauchy Horizons

RESEARCHER: Professor Deborah A. Konkowski
SPONSOR: National Science Foundation (NSF)

Deborah A. Konkowski is studying spacetimes with mild singularities and Cauchy horizons. 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, D. A. Konkowski is studying (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. Preliminary results were presented at the 4th Eastern Gravity Meeting (April 2000) and the American Physical Society's April 2000 Meeting.

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, which occur in the plane wave and exact mass-inflation spacetimes. Results on this work were published in the journal *Classical and Quantum Gravity* and later presented at the 9th Midwest Geometry Meeting (Nov. 1999) and the 9th Midwest Relativity Meeting (Nov. 1999).

In the third case, spacetimes with nonscalar and quasiregular singularities are under investigation. 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.

The Mathematical Properties of Entanglement

RESEARCHER: Associate Professor Robert B. Lockhart
SPONSORS: Naval Academy Research Council (NARC) and Naval Research Laboratory (NRL)

One of the most useful properties a quantum system can have from the point of view of quantum computation is entanglement. An entangled system has a given property such as spin as a system, but the individual particles comprising the system do not have the property. However, after a measurement is made all the particles have the property. One can use this in many ways and so it is important to be able to decide when a system is entangled and to classify all entangled states among all density states.

Developing Analytical Methods for the Navy's Antenna's EM Propagation and Interactions Program

RESEARCHER: Professor Peter A. McCoy
SPONSOR: Office of Naval Research (ONR - Code 313),
Surveillance, Communications and Electronic Combat Division

The investigator constructed an integral transform and its inverse, which associate solutions of the scalar Helmoholz equations with analytic functions of one complex variable. These representations are used to specify surfaces containing the sources or targets from an analysis of the radiation patterns. The investigator developed integral transforms for the study of scattered electrical fields. Representations of this type are necessary for the development of sampling methods for approximating electrical fields in terms of discrete sets of sampled frequencies. Based on these results, two papers were written: one for acoustic problems and the other in electromagnetic.

The Object/Image Equations of N Lines

RESEARCHERS: Professor George Nakos (USNA) and Robert Williams (NAWC)
SPONSORS: Naval Academy Research Council (NARC)
and Naval Air Warfare Center (NAWC)

The problem of recognizing an object from a two-dimensional picture is central in Computer Vision. For example, a Navy pilot takes a picture of an object and wants to identify it based on certain key line features against a database of two-dimensional images of similar objects. An example of a shape that is relevant here is that of a ship. If we assume that a set of lines (possible on a three-dimensional object) 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 the object/image equations. It is usually assumed that both the object points and the image points are determined up to a rotation and a translation prior to projection. We actually allow the object and its image to be determined up to slightly more general transformations. This project seems similar to the previous one but this time the object/image equations for lines are far more complicated that the case of points. In fact, to get the equations for a set of six lines required the efforts of several mathematicians over a period of approximately three years. In this paper we generalize the results for n lines. The equations are very complicated but can be described by using Cramer's rule type of notation. This paper extends results of Turner, Williams, Grosshans, and Gleason. This paper is currently prepared to be submitted for publication.

Shifts on Operator Algebras

RESEARCHER: Professor Geoffrey L. Price
SPONSORS: National Security Agency (NSA) and 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 hyper finite 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 bit stream of 0's

and 1's, which defines the shift. The structure of the shift is reflected in certain properties possessed by the bit stream, the most conspicuous of which is whether or not the bit stream is eventually periodic. In fact, the bit stream is eventually periodic if and only if there is a finite positive integer k such that the kth power s^k of the shift s has range $s^k(R)$ with nontrivial relative commutant in the hyper finite 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 endomorphism 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 endomorphism 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 endomorphism a_t, $t > 0$, is trivial. Using the theory of Markov semigroups Price is at work on constructing new examples of shifts on the von Neumann algebra B(H).

Naval Applications of the High Level Architecture's Run-Time Infrastructure

RESEARCHER: Professor Thomas J. Sanders
SPONSOR: Naval Research Laboratory (NRL)

The DoD Modeling and Simulation Master Plan [DoD95] calls for the establishment of a DoD wide high level architecture (HLA) for modeling and simulation. The purpose of this is to facilitate interoperability among simulations and to promote the reuse of simulations and components. The Defense Modeling and Simulation Office (DMSO) was the leader in the development of the HLA. The HLA was adopted as the Facility for Distributed Simulation Systems 1.0 by the Object Management Group (OMG) in November 1998. The HLA is now in the process of becoming an open standard through the Institute of Electrical and Electronic Engineers (IEEE). The objective of this study was stated as follows. The High Level Architecture's (HLA) Run-Time Infrastructure (RTI) shall be examined for Naval applications at NRL. It is desired that metrics for naval operational scenarios be developed and evaluated utilizing naval simulation systems. Appropriate metrics for the RTI shall be determined and described for slower-than- real-time, real-time, and faster-than-real-time federations. Measurement systems and methods shall be developed to quantify these metrics based upon a set of standard scenarios. Appropriate tests will be developed in cooperation with other NRL and NUWC personnel to gather performance data during execution of these scenarios on various simulation hardware and software systems.

The HLA allows the combining of several simulations, called federates, into one large simulation, called the federation. The HLA manages the communication of changes in parameters and interactions between federates. The principal metrics chosen for this study were latency and throughput. Latency was defined as the time delay between the publication of a change by a federate and the receiving of notification of the change by another federate. Throughput was defined as the rate of message units transfer.

DMSO provides a number of benchmark testing programs. For most platforms, this includes programs for measuring two-way latency and throughput. Agreement was reached between the investigator, Paul Maassel and Frank Segaria of NRL to use these programs to examine the latency and throughput of five different platforms. These platforms are as follows: SGI (IRIX 6.2 operating system), Sun Ultra-2 (solaris operating system), Sun SPARCstation-20 (solaris operating system), Windows NT and Windows 98. The benchmark latency program works by setting up two federates. The sender federate generates a change in a parameter by setting its value to the current time. It then sends out notification of the change. The reflector federate receives the notification and resends the parameter. When the sender federate receives notification of the reflector's receipt, the difference between the time the original change was sent and the time the last notification was received is calculated and recorded. This difference is called the two-way latency. It consists of 3 separate time intervals: message from sender to reflector, delay at reflector before resending, and message from reflector to sender. Dividing the two-way latency by 2 gives the average one-way latency.

Runs were made and data collected with each of the 5 platforms running the RTI executive program rtiexec and each of the 5 platforms running the send and reflect federates, for a total of 25 test combinations. For many of the combinations, several runs were made. Results are available on request.

Differential Simplicity and Tight Closure

RESEARCHER: Assistant Professor William N. Traves
SPONSORS: Natural Science and Engineering Research Council of Canada (NSERC)
and Naval Academy Research Council (NARC)

Grothendieck showed that the ring of differential operators on a smooth complex algebraic variety is always generated by derivations. In prime characteristic this fails, even for Euclidean space. The main thrust of the first part of this project was to extend Grothendieck's theorem to arbitrary characteristic by introducing the Hasse-Schmidt derivations. Along the way, Professor Traves showed the Hasse-Schmidt derivations extend over e'tale extensions, generalizing results due to Brown and Kuan and, separately, Ribenboim. Professor Traves also found a counterexample to an old question posed by Brown and Kuan: do Hasse-Schmidt derivations localize? Their conjecture can be reformulated in terms of the Hasse-Schmidt algebra.

In the second part of this project, Professor Traves showed that, under mild conditions excellent differentially simple rings determine (pseudo-) rational singularities in prime characteristic. The proof uses the theory of tight closure and techniques pioneered by Smith in the study of D-simplicity. In particular, he showed that the test ideal is differentially stable. This material was accepted for publication in the *Journal of Algebra*.

Near Field Closed Loop Degaussing by Moment Correlation

RESEARCHER: Professor John C.Turner
SPONSOR: Naval Systems Weapons Center (NSWC)

This classified report discusses results in Near Field CLDG. These results were tested in a small scale sea trial and found to be satisfactory for future work.

Electromagnetic Signature Reduction

RESEARCHERS: P. Izat and and Professor John C. Turner (USNA)
SPONSOR: David Taylor Research Center (DTRC)
Naval Surface Warfare Center, Annapolis (NSWC/A), Code 851

The past year has been devoted to preparing for the third phase of this project. This has involved developing new algorithms. These will be tested in sea trials in June-July 2000.

Image Recognition Problems

RESEARCHERS: Professor Peter R. Turner (USNA) and Robert M. Williams, Naval Air Warfare Center (NAWC)
SPONSORS: Naval Air Warfare Center (NAWC), Office of Naval Research (ONR) and
Naval Air Warfare Center (NARC)

Growing out of earlier work for NAWC, the problems of image recognition and moving object location in computer vision were studied using a linear algebra and vector-geometric approach. This yielded a simple approach to the solution of the image recognition problem and for the application of this same algorithm to the problem of locating (in three-dimensional space) an object from two-dimensional images.

Independent Research

Integrating Image Processing Research into the Undergraduate Mathematics Major Curriculum

RESEARCHER: Professor Carol G. Crawford

This ongoing research extends prior work by the author in the area of state-of-the-art applications of graph theory to real world problems in image processing and computer vision. These topics are based on the author's funded research 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 major focus of this research effort has been the design of classroom implementations of applied graph theory. These applications include graph representations for robot vision systems design and graph representations of fingerprint minutiae maps for neural networks matching and classification of fingerprint images. These applications utilize major concepts from mathematics courses such as Matrix Theory, Linear Algebra, Analysis and Discrete Mathematics I and II.

Using Pulsars for Orbital Velocity and Position

RESEARCHERS: Professor W. J. Bagaria (Aerospace Engineering Department)
and Associate Professor Sonia M. Garcia (Mathematics Department)

Pulsars that are in the Milky Way Galaxy can be used for orbital velocity and position determination. However, the pulsar signal is about 10 orders of magnitude lower than the background noise. Vibration techniques, such as cross-correlation, are being proposed as means to detect the pulsar signal, and the associated Doppler shift in near real time. Once the signals from three or more pulsars are measured in near real time, the velocity and position of an object, like the earth, can be determined. The signals from pulsars are periodic pulses. Because the signal level is very low compared to the background noise of space, classic signal processing procedures to detect and analyze the signal require averaging the signal over a period of several months to several years. Using these classical techniques, it has been determined that the period of the pulses is stable to one part in 1014.

In order to use the pulsar signals for orbital velocity and position determination, it is necessary to receive signals from at least three pulsars, and to determine the change in the signal period due to the Doppler shift that arises from the Earth's motion about the sun, and the receiving antennas rotation about the Earth's spin axis. The Earth's average velocity about the sun is 30 km per second, and the maximum surface velocity of the Earth due to its rotation is about 1,600 km per hour. The Doppler shift due to the orbital velocity is on the order of milliseconds, whereas that due to the rotational velocity is on the order of micro-seconds. Thus, it is necessary to analyze the pulsar signal based on as short of a time as possible. Preliminary tests have been conducted using existing lab equipment. Signals for duration of about two minutes have been captured, digitized and stored. Custom software programs have been written, by Professor Ratcliffe, to extract the pulsar signal from the background noise. This was done by using a unique random signal cross correlation technique. The noisy raw Doppler shifted signal was cross-correlated to the known pulsar signal, which does not contain the Doppler shift. In this manner, the Doppler shift due to the Earth's orbital motion was recovered.

The purpose of this research is to put the technique on firmer mathematical bases, and to gather more data so that the process, including the computer programs, can be modified and refined. To this end, new lab equipment is on order. The ultimate objective would be to automate the system, so that orbital position and velocity can be determined on quasi- real time bases. If this can be accomplished, the position and velocity of any orbiting object could be determined. The preliminary signal extraction technique and computer program is due to Professor Ratcliffe. The preliminary cross-correlation theory is due to Professor Bagaria. The detailed mathematical analysis, and refinements will be performed by Professors Garcia and Bagaria.

Classification of Nilpotent Groups

RESEARCHER: Professor Anthony M. Gaglione

The classification of finitely generated nilpotent groups up to isomorphism is an old and very challenging problem. I have been working on this in collaboration with two other professors; one from Philadelphia, PA and the other from New York, NY. We have been investigating three avenues of attack for this problem. Each of these leads in itself to other problems of independent interest and of importance. The avenues of investigation are (I) the genus problem for nilpotent groups (this has important connections to topology), (II) the rigidity problem, and finally the related problem (III) direct decomposability (or "reducibility") for nilpotent groups.

A Posteriori Error Estimation for Parabolic Equations using Mixed Finite Element Method

RESEARCHERS: Dr. Carsten Carstensen (University of Kiel, Germany)
and Associate Professor Sonia M. Garcia

It is part of this joint work to develop and implement accurate approximation methods for differential equations using a posteriori error estimates and adaptive error control. The main target are systems of reaction-diffusion equations. Such problems are important in practical terms because they occur as mathematical models in applied science and engineering, including applications in genetics, material science, chemistry, and biology, among others. The challenge is to compute accurate approximations of solutions that generically include multiple scales in their space and time behavior and whose behavior depends strongly on parameters prescribed as part of the model. Moreover, using computation as a scientific tool requires an estimate of the accuracy of the approximation. The approach to these problems is based on developing a posteriori error estimates that bound the error in terms of computable information obtained from the approximation once a computation is completed. Let u in H be the exact solution of a given problem, which is approximated by some u_S in S, S being a suitable finite element space. Efficient and reliable a posteriori estimates of the error $||u-u_S||$, measuring the (local) quality of u_S, play a crucial role in termination criteria and in the adaptive refinement of the underlying mesh.

In-Class Projects and Group Exercises for Calculus

RESEARCHER: Professor Charles C. Hanna

Professor Hanna is planning to create approximately 50 one- or two-page projects to accompany calculus I and calculus II. Each project will be designed for in-class work, usually by small groups of midshipmen, taking 10-30 minutes. Most will focus on using calculators or computer programs to enhance understanding of the basic ideas of calculus. Many will include careful instruction in various features of the TI-89/TI-92+ calculators. The plan is to extract this material and assemble it on a web site as a potentially useful reference for midshipmen and instructors.

During the 2001 Academic Year, Professor Hanna created and used 54 of these projects. The 36 calculus I projects and 32 small calculator tutorials are also available through the Mathematics Department website. (See http://www.usna.edu/MathDept/website/Courses/ComputersCalculators/Hanna/GuideIndex.htm.)

Einstein Gravitational Fields and their Relation to a Classical Electromagnetic Zero Point Field

RESEARCHER: Professor Robert A. Herrmann

Using aspects of nonstandard analysis and the concept of potential velocities, the Einstein gravitational field that yields the Schwarzschild metric is correlated to the conjectured classical zero-point electromagnetic field (ZPF) via the infinitesimal light clock. These results give yet more theoretical evidence that gravitational effects are closely related, if not actually produced by, the ZPF.

Basic Examples of Goppa Codes for Varieties

RESEARCHERS: Professor W. D. Joyner and Assistant Professor William N. Traves

This project investigates the construction and properties of Goppa codes - methods to encode data for fast and accurate transmission across a noisy or unstable channel. These cosed 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.

Multiplicity One for SL(2)

RESEARCHERS: Professor David D. Joyner, Associate Professor Courtney H. Moen, and Jason Levy (U. of Waterloo)

We apply 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 is a multiplicity one theorem for most automorphic representations of SL(2), where A denotes the ring of adeles of a totally imaginary number field.

Number Theory and Tiling

RESEARCHER: Associate Professor Courtney H. Moen

I have continued to work on various problems in tiling and number theory. In particular, I have proved a result, which is a step in the direction of proving a difficult conjecture concerning the tiling of squares. The dissection of squares into unequal squares has a long history. Various methods have produced many such dissections, but there appears to have been no work done on the question of which squares can be dissected into unequal squares. A similar problem is to determine which squares can be dissected into unequal rectangles of size n-by-(n+1). After much evidence was gathered, it was conjectured that any square of even side greater than 14 could be dissected into unequal rectangles of this shape. The result that I have proved is that any square of even side greater than 14 can be dissected into squares and rectangles of size n-by-(n+1), no two of these being identical. I am presently writing up this result for publication. Two short papers I submitted last year appear to have been lost and are being resubmitted. One is an expository paper concerning the dissection problem mentioned above. The other concerns a generalization of a classical problem of Kaprekar concerning digital permutations. The idea for this paper arose as I was explaining Kaprekar's problem to Midshipman 1/C Holsten, who wrote his SM332H capstone paper on this topic.

Classification of Singularities with SHEEP/CLASSI

RESEARCHER: Professor Deborah A. Konkowski

Deborah A. Konkowski 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.

A Numerical Algorithm For a Class of Integro-Differential Equations

RESEARCHER: Professor Thomas J. Mahar

The investigator developed a program to construct numerical solutions to a class of integro-differential equations motivated by a problem for a visco-plastic material. The discrete equations were shown to have qualitatively correct solutions for

several kernel functions. A class of integro - partial differential equations were shown, analytically, to be unstable, with the instability originating in the higher modes, even though the corresponding integro-ordinary differential equations were exponentially stable. Numerical simulations verified this analysis.

Single-Step Combinatorial Resolution via Coherent Sheaves of Ideals

RESEARCHERS: Associate Professor Caroline Grant Melles (USNA) and
P. Milman (University of Toronto)

We considered complex analytic varieties whose singularities may be resolved by a finite sequence of blow-ups along smooth centers, each of which is an intersection of smooth normal crossings divisors, arising either as strict transforms from the base space or as exceptional divisors from previous blow-ups. We gave an algorithm for replacing such a sequence of blow-ups by a single blow-up along a coherent sheaf of ideals which is locally generated by monomials in appropriate coordinates.

A paper based on these results has been accepted for publication in the Proceedings of the Conference of Singularities in Algebraic and Analytic Geometry, San Antonio, TX, 1999, to be published by the AMS.

Functions in Generalized Pinchuk Classes

RESEARCHER: Associate Professor Edward J. Moulis

Let N be the set of all 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 which consist of those functions in N defined by their satisfying, with J(f)=1-1/c + (z/c)*(f=/f), z = r e^(it), 0 ≤ r < 1, c a non-zero complex number and -Pi/2<L<Pi/2, 0 ≤ b < 1 and k ≥ 2 we have [MAPLE] 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) named after this researcher who introduced the basic class V(k,0,0,L) in his Ph. D. thesis. We try to find sharp bounds, in terms of the parameters k, b, L (all real) and the complex number c, for geometric mapping properties of functions in these classes, including distortion bounds on |f(z)| , |f=(z)|, rotation bounds on |arg f(z)| as well as bounds on the moduli of the series coefficients a(n).

Polynomial Partitions in the $[p^k]$ -series

RESEARCHER: Professor George Nakos

In recent years there has been renewed interest in Dr. Nakos' PhD thesis work. This work mentioned several times at the recent Conference in Homotopy Theory at the Johns Hopkins University in the Spring. An effort has been made to extend Dr. Nakos' study on the $[p^k]$ -series, a homotopy theory encoding series that carries all the information of the bordism of finite abelian groups. Recently, Jesus Gonzalez has made a study of the p-divisibility of the coefficient of the $[p^k]$ -series, based on ideas of earlier work of Nakos. Using these results he has found new nomimmersions of lens space in the Euclidean space.

In the present work Nakos uses some old ideas (paper written with Nick Glinos) to vastly generalize Gonzalez's results on the $[p^k]$ -series. One of the great features of the Nakos/Glinos paper was in fact a closed form solution of the coefficient of the series. This formula had not been previously noticed (and thus not appreciated) by area experts. This paper is currently prepared to be submitted for publication.

Nakai's Conjecture for Varieties Smoothed by Normalization

RESEARCHER: Assistant Professor William N. Traves

This paper appeared in the Proceedings of the American Mathematical Society. Nakai's conjecture concerns a very natural question: can differential operators detect singularities on algebraic varieties? On a smooth complex variety, it is well known that the ring of differential operators is generated by derivations. Nakai asked whether the converse holds: if the ring of differential operators is generated by derivations, is the variety smooth? In this paper, the notion of D-simplicity is used to give

a short proof that varieties whose normalization is nonsingular satisfy Ishibashi's extension of Nakai's conjecture to arbitrary characteristic. This yields a new characteristic-free proof of Nakai's conjecture for curves. The argument is concise and rederives characteristic dependent results of Mount and Villamayor (characteristic zero) and Ishibashi. The argument also provides a new proof of Nakai's conjecture for Stanley-Reisner rings and, more generally, unions of smooth varieties. The proof plays off Hasse-Schmidt stability against D-simplicity in a subtle way.

An Invitation to Algebraic Geometry

RESEARCHERS: Assistant Professor William N. Traves (USNA),
Karen Smith, University of Michigan and M.I.T.
Lauri Kahanpaa, University of Jyvaskula , Finland
and Pekka Kekalainen, University of Jyvaskula, Finland

This book has been accepted for publication by Springer-Verlag in the Universitext series. The book consists of a gentle introduction to Algebraic Geometry intended for senior mathematics majors or first-year graduate students. Initially dealing with geometric objects defined by polynomial equations, we develop the standard dictionary between algebraic and geometric objects. Schemes and abstract varieties are introduced, but in order to maintain readability, pathologies are avoided. Many central topics are treated: there is an entire chapter on birational equivalence and resolution of singularities, vector bundles are introduced, and moduli spaces make an appearance. Our intention in writing this book was to give an overview of the subject and to provide students with a context in which to understand research work in Algebraic Geometry.

Clique Polynomials

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

Clique polynomials occur naturally in a counting problem involving words in a partially commutative alphabet. They also occur in recent work by Allan Sokal on the Pott's model in statistical physics; indeed, Sokal's work suggests that clique polynomials may be closely related to chromatic polynomials of graphs. Motivated by research on chromatic polynomials, we locate the roots of the clique polynomials in the complex plane. Though the possible locations form a dense subset of the complex plane, the roots of special classes of clique polynomials exhibit interesting structure. Using certain special constructions, we were able to produce a counterexample to a conjecture of Brown, Dilcher and Nowakowski. They conjectured that the coefficients of clique polynomials associated to well-covered graphs are unimodal. Using techniques from combinatorial set theory, we were able to verify their conjecture for the first half of the coefficients, though the behavior of the remaining coefficients seems to be unconstrained. This research is ongoing. Portions of our work are currently being prepared for publication.

Maple and Mathematica for Computations

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 am also studying the problem of the existence of normed bilenear 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.

SM230 Textbook

RESEARCHER: Professor John C. Turner

The revision of the SM230 textbook continues. In response to requests from other departments, Professor Turner included some statistical concepts. Both confidence intervals and hypothesis testing are introduced. Unlike other texts, this material is introduced at the same time the associated probability topic occurs. This emphasizes the connection between statistics and probability. It also tries to avoid statistics becoming a sequence of formulas to be memorized.

Implementation and Applications of Level-index Arithmetic

RESEARCHER: Professor Peter R. Turner

This project continues the development of possible schemes for the eventual hardware implementation of SLI arithmetic and the analysis of the algorithms used. We also are gaining more computational experience and evidence of the potential practical value of the system using software implementations of the symmetric level-index, SLI arithmetic system. This was a continuation of previous work on the level-index system. The recent activity has centered on the study of the effect of using SLI arithmetic with Ulam's shift map. This map is widely studied in Chaos Theory. It performs completely differently on the binary floating-point based computer than the mathematical theory suggests. Using SLI arithmetic the behavior is qualitatively similar to that which is predicted.

The RSA Public Key Cipher Algorithm

RESEARCHER: Professor William P. Wardlaw

In May and June 1999, after making my expository presentation of "The RSA Public Key Cipher Algorithm" at the U. S. Naval Academy Conference on Cryptography and Coding Theory on 26 October 1998, Professor Wardlaw wrote a more extensive version of the material for publication in the conference proceedings.

A Generalized General Associative Law

RESEARCHER: Professor William P. Wardlaw

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-associative implies $(n + 1)$-associatively when $n > 2$. The paper is now being revised to conform to suggestions of referees for *Mathematics Magazine*.

Research Course Projects

The Jeep in a Graph Problem

RESEARCHER: Midshipman 1/C Craig Matthew Trent, USN
ADVISER: Associate Professor T.S. Michael

This is Midshipman 1/C Trent's Honors project. We pose the discrete version of a famous optimization problem and prove theorems about optimal schemes for delivering messages in a network subject to cost constraints. We encountered surprisingly complicated behavior embedded in a simple discrete situation. We are preparing this work for publication.

A Labeling Problem on Circular Permutations

RESEARCHER: Midshipman 4/C Todor E. Milev, USN
ADVISER: Associate Professor T.S. Michael

Suppose we have *n* beads that are labeled with the integers 1,2, ... , n. We arrange these beads in a random order in a circle to form a circular permutation *P* and then look at the *n* sums formed by triples of consecutive beads. Denote the largest such triple sum by S(P). What is the minimum value of S(P) as P varies over all circular permutations of the beads. In fact, one can show that $M_{10} = 18$ by a clever counting argument. For the case of general n we have asymptotic upper and lower bounds for M_n.

Solution to a Problem in the American Mathematical Monthly

RESEARCHER: Midshipman 4/C Todor E. Milev, USN
ADVISER: Associate Professor T.S. Michael

Problem # 10774 (Jan 2000) : Let F(1) = F(2) = 1 and F(n) = F(n-1) + F(n-2) for N≥3.

Show F(1998)))2+(F(F1999)))2=F(F(1997))F(F(2000)).

We have produced a generalization with a solution to this problem and are submitting it for publication.

Fractals

RESEARCHER: Midshipman 1/C Evelyn Melo, USN
ADVISER: Professor W. D. Withers

A *fractal* is a geometric figure whose structure repeats on infinitely many scales. The complexity of fractals persists on closer and closer examination. This differs from the differentiable curves of calculus whose structure resembles a straight line when studied up close. The researcher studied the use of *iterated function systems* to generate fractals. General properties of metric spaces were used to derive the properties of the fractal space, a metric space whose individual points represent sets in another complete metric space. Proof that the fractal space is complete allowed the use of the fixed-point theorem to show that every iterated function system generates a unique fractal set.

Publications

BOLLT, Erik, Associate Professor, and Michael A. Jones, "Developing Symbolic Dynamics to Measure the Complexity of Repeated Game Strategies by Topological Entropy," Nonlinear Dynamics, Psychology, and Life Sciences, 4 2 153-168, 2000.

State spaces, directed graphs, and transition matrices are implemented to consider sequences of play of repeated games as a dynamical system on the symbol space, defined as the outcomes of the stage game. Strategies are described as subshifts of this symbol space. The complexity of bounded recall strategies is equated with the topological entropy of an associated transition matrix. The topological entropy measures how complicated a strategy is by what paths of the extensive form game are possible under the strategy. This measure is used to compare the complexity of different strategies.

BOLLT, Erik, Associate Professor, R. Davidchack, Y-C Lai, and M. Dhamala, "Estimating generating partitions of chaotic systems by unstable periodic orbits," Physical Review E, 61 2 1353-1356, 2000.

An outstanding problem in chaotic dynamics is to specify generating partitions for symbolic dynamics in dimensions larger than one. It has been known that the infinite number of unstable periodic orbits embedded in the chaotic invariant set provides sufficient information for estimating the generating partition. Here we present a general, dimension-independent, and efficient approach for this task based on optimizing a set of {\it proximity} functions defined with respect to periodic orbits. Our algorithm allows us to obtain, for the first time, the approximate location of the generating partition for the Ikeda-Hammel-Jones-Moloney map.

BOLLT, Erik, Associate Professor, "Stability of Order: An Example of Horseshoes "Near" a Linear Map," International Journal of Bifurcation and Chaos, Vol. 9, No. 10, Oct 1999.

We have been motivated by a question of "anti-control" of chaos [Schiff {\it et al.}, 1994], in which recent examples [Chen \& Lai, 1997] of controlling nonchaotic maps to chaos have required large perturbations. Can this be done without such brute-force? In this paper, we present an example in which a family of maps, G_ϵ, numerically displays a transverse homoclinic point, and hence a horseshoe and hence chaos, for a fixed value of the parameter ϵ. We show that these maps converge pointwise to a linear map. Furthermore, a simple scaling conjugacy is shown for a family of maps which even gives geometric similarity of all relevant structures. This is in seeming contradiction to well known structural stability results concerning horseshoes, but careful consideration reveals that these theorems require convergence in a uniform topology in function space. We show that no such convergence is possible for our family of maps, since it is impossible to find a finite radius disk which contains all of the horseshoes Λ_ϵ for every ϵ. Thus, there is no contradiction. Our example may be considered to be a new kind of bifurcation route to chaos by horseshoes, in which rather than creating/destroying a horseshoe by creating/destroying transverse homoclinic points, the horseshoe is sent/brought to/from infinity.

BOLLT, Erik, Associate Professor, and K. Zyczkowski, "On the Entropy Devil's Staircase in a Family of Gap-tent Maps," Physica D 132 3 392-410 (1999).

To analyze the trade-off between channel capacity and noise-resistance in designing dynamical systems to pursue the idea of communications with chaos, we perform a measure theoretic analysis the topological entropy function of a "gap-tent map" whose invariant set is an unstable chaotic saddle of the tent map. Our model system, the "gap-tent map" is a family of tent maps with a symmetric gap, which mimics the presence of noise in physical realizations of chaotic systems, and for this model, we can perform many calculations in closed form. We demonstrate that the dependence of the topological entropy on the size of the gap has a structure of the devil's staircase. By integrating over a fractal measure, we obtain analytical, piece-wise differentiable approximations of this dependence. Applying concepts of the kneading theory we find the position and the values of the entropy for all leading entropy plateaus. Similar properties hold also for the dependence of the fractal dimension of the invariant set and the escape rate.

BOLLT, Erik, Associate Professor, "Controlling Invariant Density: An I^{00} Solution to the Inverse Frobenius-Perron Problem," to appear ISCAS'2000, Conference Proceedings, Geneva, Switzerland, May 2000.

In a previous paper, \cite{IFFP-bollt}, we gave a new formalism to solve the Inverse Frobenius-Perron Problem (IFPP), to produce a dynamical system, uniformly nearby a given dynamical sytem, but with a drastically different and desirable invariant density. Our previous algorithm reduced the problem of producing the dynamical system G with desirable statistics $\beta(x)$, into a constrained optimization problem, which we solved in l^2. However, we pointed out that if this l^2 solution does not correspond to a useful solution, one could not conclude nonexistence. The l^∞ solution to the same optimization problem allows for a sharp existence-nonexistence theorem. In this paper, we present for the first time an l^∞ algorithm which produces solutions to our IFPP, and conclude our nonexistence theorem which is pertinant to this solution. Then we discuss applications in control of chaos, both by open-loop control strategies for maps, and we discuss future applications to feedback control of flows.

BUCHANAN, James L., Professor, R.P. Gilbert and A. Wirgin, "Finding an Inclusion in a Shallow Ocean Using the ICBA Method." *Applicable Analysis*, 71, 347-78, 1999.

BUCHANAN, James L., Professor, R.P. Gilbert, A. Wirgin, and Y. Xu, "The Unidentified Object Problem in a Shallow Ocean with a Fluid-like Sediment Layer Overlying a Rigid Seabed," *Applicable Analysis*, 73, 5-17, 1999.

GAGLIONE, Anthony M., Professor, (co-author), "Aspects of the Theory of Non-Abelian Free Groups: Algorithmic Problems in Groups and Semigroups," (2000) 51-90.

Combinatorial (or Infinite) Group Theory refers to the theory of group presentations, that is, of groups specified by a set of generators and corresponding defining relations. The theory has its origins in topology and complex analysis and in particular in the theory of the fundamental groups of combinatorial cell complexes. Because of its nature and its origins, combinatorial group theory comes into contact with and uses many different areas of mathematics. Clearly algebra and topology as mentioned are very significant for the combinatorial group theorist. But also hyperbolic geometry comes into play via the study of Cayley graphs, pure mathematical logic through the study of various decision problems, and last, but not least, computer science through the study of rewriting systems (Certain kinds of algorithms). Central to all of these studies is the concept of a free group. This centrality is due to the fact that a free group is the most basic construction of infinite group theory and also that free groups serve as primary motivating examples for both properties and proofs in all the other areas mentioned. The purpose of this paper was to try to bring to bear all these different points of view and focus primarily on the group theoretical properties closely tied to the Tarski conjecture. This conjecture has to do with the relations of combinatorial group theory to pure logic and the logical underpinnings of the whole theory. This conjecture has now been settled by one of the co-authors of this paper, as we report here.

HERRMANN, Robert A., Professor, "The NSP-world and Action-At-A-Distance," in Instantaneous Action at a Distance in Modern Physics Pro and Contra Edited by Chubykalo, A., N. V. Pope and R. Smirnov-Rueda, (In the series CONTEMPORARY FUNDAMENTAL PHYSICS B V. V. Dvoeglazov (Ed.)) Nova Science Books and Journals, New York 1999.

Using the Nonstandard Physical World (NSP-world) model, a model that cannot be eliminated from scientific discourse, it was predicted that specific processes exist such that information between objects within our natural environment would appear to be transmitted instantaneously. In this article, certain aspects of this model are discussed as well as experimental evidence that establishes as fact the model's prediction that a type of nonlocal instantaneous action-at-a-distance does occur in objective reality.

HERRMANN, Robert A., Professor, Information Theory, Consequence Operators, and the Origin of Life, CRS Quarterly, 36(3) (1999) 123-132.

In this article, the Gitt (1997) concept of information as it is represented by a mental-like sequence of activities is compared with the mental activity represented by consequence operators. It is shown how consequence operators

model mathematically these Gitt notions and how a specific ultralogic and four ultrawords yield an identical foundation for Gitt's information theory scenario for the origin of life. Consequence operator theory, as a model for Gitt information theory, is used to establish that, relative to this model and without external modification to the processes, it is not possible, using fixed pragmatic information, to increase or decrease the complexity of a biological entity by selecting from two distinct independently produced biological entities as these entities are characterized at the apobetic level. This signifies that if random mutations are random alterations in the characteristics of a biological entity that are, necessarily, not dependent upon the original biological characteristics, then this model would tend to disallow random mutations as a viable source for biological alterations. On the other hand, for fixed pragmatic information, an increase or decrease in complexity by selecting from two distinct pobetic level biological entities is possible if a very special dependency exists between their characteristics. Further, complexity can also be increased by applying the semantic level consequence operator to an increased portion of the information contained within the generic code in DNA, information that exists originally.

HOFFMAN, Michael, Professor, "Quasi-shuffle Products," Journal of Algebraic Combinatorics, 11 (2000), 49-68.

Given a locally finite graded set A and a commutative, associative operation on A that adds degrees, we construct a commutative operation * on the set of noncommutative polynomials in A, which we call a quasi-shuffle product; it can be viewed as a generalization of the shuffle product. We extend this commutative algebra structure to a Hopf algebra; in the case where A is the set of positive integers and the operation on A is addition, this construction gives the Hopf algebra of quasi-symmetric functions. If rational coefficients are allowed, this construction is in fact no more general than the shuffle product; we give an isomorphism exp from the shuffle Hopf algebra on A to the quasi-shuffle Hopf algebra on A. Both the set L of Lyndon words in A and their images under exp freely generate the quasi-shuffle algebra on A. We define a deformation *q of * that coincides with * when q=1 and is isomorphic to the concatenation product when q is not a root of unity. Finally, we discuss various examples, particularly the algebra of quasi-symmetric functions (dual to the noncommutative symmetric functions) and the algebra of Euler sums.

JOYNER, David, Professor, "A Correspondence for the Supercuspidal Representations of the Metaplectic Cover of SL(2,F), F p-adic," Archiv der Math, vol 73 (1999) 332-340.

Following D. Manderscheid, we describe the supercuspidal representations of the n-fold metaplectic cover G of SL(2,F), where F is a p-adic field with p not dividing 2n. We prove a "Frobenius formula" for the character of a supercuspidal representation of G. Using this formula, we obtain a character relation between corresponding supercuspidal representations of G and of SL(2,F)$ in the case n=2.

JOYNER, David, Professor, "Coding Theory and Cryptography: From Enigma and Geheimschreiber to Coding Theory," editor, (Springer-Verlag).

These are the proceedings of the Conference on Coding Theory, Cryptography, and Number Theory held at the U.S. Naval Academy during October 25-26, 1998. This book concerns elementary and advanced aspects of coding theory and cryptography. The coding theory contributions deal mostly with algebraic coding theory. Some of these papers are expository, whereas others are the result of original research. The emphasis is on geometric Goppa codes, but there is also a paper on codes arising from combinatorial constructions. There are both, historical and mathematical papers on cryptography. Several of the contributions on cryptography describe the work done by the British and their allies during World War II to crack the German and Japanese ciphers. Some mathematical aspects of the Enigma rotor machine and more recent research on quantum cryptography are described. Moreover, there are two papers concerned with the RSA cryptosystem and related number-theoretic issues. Keywords: coding theory, cryptography, rotor ciphers.

JOYNER, David, Professor, with Salahoddin Shokranian, "Remarks on Codes from Goppa Curves: MAPLE applications," in "Coding Theory and Cryptography: From Enigma and Geheimschreiber to Coding Theory," pp. 229 – 250, Springer-Verlag, 2000.

We are going to restrict our attention in this paper to the interplay between Goppa codes of modular curves and the problem of counting points on a curve over a finite field, and give some examples using MAPLE, where the programs

using for the calculation are written in MAPLE by the first named author. In coding theory, curves with many rational points over finite fields are being used for construction of codes with some good specific characteristics. We discuss the Goppa codes, first from an abstract general perspective then turning to concrete examples associated to modular curves. We will try to explain these extremely technical ideas using a special case at a level to a typical graduate student with some background in modular forms, number theory, group theory, and algebraic geometry.

KONKOWSKI, Deborah A., Professor (co-author), "Testing a Stability Conjecture with Plane-wave Cauchy Horizons," Class. Quantum Gravity 16 (1999) 2709-2728.

Plane-wave Cauchy horizons serve as an important testing ground for a previously developed Cauchy horizon stability conjecture. The conjecture uses test fields to predict the stability of Cauchy horizons in general relativistic spacetimes. Three cases are considered: single plane waves with (a) aligned test fields and (b) colliding test fields; and (c) non-singular interaction regions in colliding wave spacetimes. A restricted form of the stability conjecture is proven for case (a). The conjecture is shown to agree with arbitrary exact back-reaction solutions in this case, as long as no Weyl-tensor singularities are introduced on an initial Cauchy surface. Four examples of case (b) are analyzed; in three the conjecture agrees with exact back-reaction solutions, and in the fourth the conjecture correctly indicates instability, but misjudges the type of singularity formed. A possible reason for the disagreement is discussed. Two examples of case (c) are analyzed, in which test null dust is added to the interaction regions of a colliding electromagnetic spacetime (Bell-Szekeres) and a colliding gravitational wave spacetime (Chandrasekhar-Xanthopoulos). The conjecture is shown to agree with known exact back-reaction solutions.

KONKOWSKI, Deborah A., Professor (co-author), "Stability of Plane-Wave Cauchy Horizons," *Proceedings of the 8th Marcel Grossmann Meeting on General Relativity, Part A*, ed. T.Piran (Singapore: World Scientific, 1999) 685-687.

A stability conjecture for Cauchy horizons is discussed. The conjecture is applied to plane-wave spacetimes and a stability theorem for plane-wave Cauchy horizons is presented.

MARUSZEWSKI, Richard F., Professor, "Analytic Tableaux, PROLOG, and Systems of Nonlinear Equations", *MACE Journal*, vol 34, #1, 53-58.

MCCOY, Peter A., Professor, "Multipower Legendre Series in Several Variables," Kernel Functions & Their Applications, Saburou Saito (editor) Kluwer Academic Publishers Inc., Boston, 1999, pp. 133-140.

Nehari's theorem links the singularities of Legendre series in Cz with those of associated Taylor's series in Ct. Recently, the theory was generalized to products of powers on m Legendre polynomials in Cm. This paper continues to develop series of products of powers of Legendre polynomials in Cm.

MCCOY, Peter A., Professor, "A Function Theoretic Approach to Multivariable Sampling," Heinrich Begehr 60th Birthday Volume, G.N. Hile, editor, Applicable Analysis, nos 1-2 (1999) 153-165.

Multivariable sampling theorems are developed for which the sampling functions are raised to powers and the usual requirements are relaxed.

MCCOY, Peter A., Professor, "On the Structure of Multivariable Sampling Series," Complex Variables, Vol. 41 (1999) 1-15.

The algebraic structure of multivariable sampling series is developed in a function theoretic context.

MCCOY, Peter A., Professor, Book Review: "Wavelets and their Applications," Stefan Goedecker, Cahiers de physique, Les Presses polytechniques et universitaires remandes, EPFL, 1998, American Mathematical Reviews (99m:00014).

MCCOY, Peter A., Professor, Book Review: "Practical Time-Frequency Analysis," Wavelet analysis & its application, vol. 9, Rene Carmona, Wen Liang Hwang & Bruno Torresani, Academic Press, 1998. American Mathematical Reviews (2000a:42050).

MICHAEL, T.S., Associate Professor, "The Rigidity Theorems of Hamada and Ohmori, Revisited," Coding Theory and Cryptography: From the Geheim-schreiber and Enigma to Quantum Theory (W.D. Joyner, ed), Springer, 1999, pp 175-179.

MYLANDER, Charles, Professor, Wager, Daniel H., and SANDERS, Thomas J., Professor, *Naval Operations Research, Third Edition*, Annapolis MD, Naval Institute Press, 1999.

This textbook for Naval Academy midshipmen focuses on search and detection theory as it was developed in World War II and evolved after the war. Accessible to anyone with a mathematical background in calculus and elementary probability theory, it covers analytical decision-making, simulation techniques, and model used in determining the probability of detection. This third edition is a comprehensive update that collects in one place the basic analytical developments in naval search theory over the last fifty years, while retaining the material on search models developed in the campaigns against the submarine threat in World War II.

NAKOS, George, Professor and Williams, Robert, "Fast Calculation of the Characteristic Polynomial," Mathematica for Education and Research, Vol. 9, Issue 1, January 2001, pp. 6-12.

NAKOS, George, Professor and Williams, Robert, "Polynomial System Triangularization with the Dixon Resultant" Proceedings CSCC'99, Athens, Greece, July 99, Vol.: Modern Applied Mathematics Techniques in Circuits, Systems, and Control, pp. 45-50.

Recently, there has been renewed interest in Dr. Nakos' doctoral thesis. The thesis was mentioned at a recent Homotopy theory conference (Johns Hopkins U., Spring 2000). There is an ongoing effort to extend Dr. Nakos' study on the p-series, a power series encoding homotopy information for the bordism groups of finite abelian groups. Recently, Dr. Jesus Gonzalez studied the p-divisibility of the coefficient of the p-series, based on ideas of earlier work of Dr. Nakos. Using these results, he has found new non-immersions of lens spaces in Euclidean space.

In the present work, Dr. Nakos generalizes Dr. Gonzalez' work by using the closed form solution of the p-series. The "closed form" appeared much earlier in a paper written jointly with Dr. N. Glinos.

PRICE, Geoffrey L., Professor, "On the Classification of Binary Shifts of Finite Commutant Index," Proceedings of the National Academy of Science, 96, 1999, pp. 14700 - 14705.

Within the same setting as the article summarized above, Price obtains a complete classification up to conjugacy of the Powers shifts of finite commutant index. In this more general situation there is a correspondence (although no longer one to one) among the shifts of finite commutant index and the polynomials over the field of 2 elements, which lack a certain symmetry condition. Roughly speaking, there are 2^{k-1} Powers shifts corresponding to each polynomial over the field of two elements having no self-reciprocal factors of degree exceeding k.

PRICE, Geoffrey L., Professor, and Truitt, Glenn H., "On the Ranks of Toeplitz Matrices over Finite Fields," Linear Algebra and Its Applications, 294 (1999), pp. 49-66.

A Toeplitz matrix is a matrix with infinitely many rows and columns whose values remain constant along each of its diagonals. Let T be a skew-symmetric Toeplitz matrix with entries in a finite field. For all positive integers n let T_n be the upper n x n corner of T, with nullity $n_n = n(T_n)$. The sequence $\{n_n\}$ satisfies a unimodality property and is eventually periodic if the entries of T satisfy a periodicity condition. We compute the maximum value and the period of the nullity sequence for Toeplitz matrices of finite bandwidth. This sequence satisfies a certain symmetry condition about its maximal values. These results apply to give some information about the ranks of general skew-symmetric Toeplitz matrices with eventually periodic entries.

PRICE, Geoffrey L., Professor, "On the Classification of Binary Shifts of Minimal Commutant Index," Proceedings of the National Academy of Science, 96, 1999, pp. 8839-8844.

Let $u_0, u_1, \ldots$ be a sequence of hermitian unitary operators in a von Neumann algebra which are assumed pairwise either to commute or to anticommute, and which satisfy the further property that for any positive integer k the pair of operators u_{i+k}, u_{j+k} have the same commutation relations as do the pair u_i, u_j. If the commutation relations are sufficiently chaotic the weakly closed algebra generated by these operators is isomorphic to the hyper finite II_1 factor R. Due to the translation invariance of the commutation relations one can define a shift endomorphism s on R which satisfies $s(u_i) = u_{i+1}$ for all non-negative integers i. Endomorphism of R defined in this way are called Powers shifts. The commutant index of s is defined to be the first positive integer k such that the von Neumann sub algebra $s^k(R)$ of R has non-trivial relative commutant in R. In this paper we obtain a complete classification of the conjugacy classes of the Powers shifts of commutant index 2 by showing that there is a one to one correspondence between these shifts and the family of polynomials over the field of 2 elements which lack a certain symmetry property, namely, that these polynomials have no self-reciprocal factors of degree exceeding 1.

STANFORD, Theodore, Assistant Professor, "Four observations on n-triviality and Brunnian links," the Journal of Knot Theory and its Ramifications, Volume 9, Number 2 (2000).

TRAVES, William N., Assistant Professor, "Nakai's Conjecture for Varieties Smoothed by Normalization," Proceedings of the American Mathematical Society, 127, (August 1999), 2245-2248.

This paper deals with Nakai's conjecture characterizing the smoothness of a variety in terms of the structure of the associated ring of differential operators. A short, elegant proof is provided that establishes Nakai's conjecture for algebraic varieties with mild singularities — those varieties that can be desingularized by normalization. This implies the result for Stanley-Reisner rings and, using an extension, for semigroup algebras.

TURNER, Peter R., Professor, NAKOS, George, Professor, and Williams, R. M., *"Fraction-free algorithms for linear and polynomial equations,"* ACM SIGSAM Bulletin Vol. 31, No. 1, December 1997, Issue 122, pp. 11-19.

This report extends the ideas behind Bareiss's fraction-free Gauss elimination algorithm in a number of directions. First, in the realm of linear algebra, algorithms are presented for fraction-free LU "factorization" of a matrix and for fraction-free forward and backward substitution. These algorithms are valid not just for integer computation, but also for any matrix system where the entries are taken from a unique factorization domain such as a polynomial ring. The second part of the paper applies a fraction-free formulation to resultant algorithms for solving polynomial systems. In particular, the use of fraction-free polynomial arithmetic and triangularization algorithms in computing the Dixon resultant of a polynomial system is discussed in detail.

TURNER, Peter R., Professor, *"Guide to Scientific Computing"* (MacMillan, March 2000).

This a completely rewritten new edition of my earlier *Guide to Numerical Analysis*. The book is some 300 printed pages long and provides a gentle yet mathematically sound introduction to the main topics of scientific computing. Its chapters deal with Number Representations and Errors, Iterative Solution of Equations, Approximate Evaluation of Functions, Interpolation (polynomial and spline), Numerical Calculus (including optimization), Differential Equations and Linear Equations (including least squares approximations). There will be an Appendix on using MATLAB for scientific computing.

TURNER, Peter R., Professor,(Contributing Author) *"Handbook of Discrete and Combinatorial Mathematics,"* Kenneth H Rosen, Editor-in-chief (CRC Press, 1999). Two sections written by PRT: *Matrix Algebra* (pp 377-392) and *"Discrete Probability Computations"* (pp. 448-452).

This section covers algorithms for all the basic matrix algebraic operations and identities. Special matrices introduced are identity, diagonal, triangular and tridiagonal matrices as well as positive definite and orthogonal matrices. The basic

algebraic operations discussed are matrix arithmetic, transposition, multiplication by special matrices, scalar multiplication of vectors and inversion of matrices. A further subsection is devoted to fast multiplication algorithms for vector and parallel computers. Further subsections deal with determinants, rank and important identities and formulas.

TURNER, Peter R., Professor, "*Teaching Scientific Computing through Projects* FIE99," Frontiers in Education, Puerto Rico, November 1999. Selected as one of 10 Best Papers.

Traditional numerical methods courses face several difficulties. There is a performance problem for students who need to combine different skills. Students spend so much time mastering the details that they often miss the point as to why there is a need for scientific computing. Using projects drawn from practical situations, and a good high-level package such as MATLAB, can overcome much of this. The difficulty associated with learning scientific programming is greatly alleviated. This in turn frees more time for studying more advanced methods. The need to combine ideas from different areas makes this an ideal candidate for both team-teaching and student teamwork on projects. In this paper, we discuss the use of this approach in a variety of scientific computing courses at different levels.

WARDLAW, William P., Professor, "The RSA Cryptosystem," *Coding Theory and Cryptography*, Springer Verlag, Berlin, 2000, pp. 101-123.

This extension of the author's presentation at the U. S. Naval Academy Conference on Cryptography and Coding Theory on 26 October 1998 begins with some elementary number theory and continues with a complete description of the Rivest-Shamir-Adelman (RSA) cipher algorithm. It concludes with some comments on the security of the RSA cipher.

WARDLAW, William P., Professor, and Michael, T.S., Associate Professor, Problem 1579, *Mathematics Magazine*, vol, 72 no. 4 (October 1999) p. 325.

For each positive integer n, find a set of positive integers whose sum is n and whose product is as large as possible.

(If repetitions are allowed with $n = 1979$, we obtain problem A-1 from the l979 Putnam Competition.)

Technical Reports

TURNER, Peter R., Professor, NAKOS, George, Professor, and Williams, R. M., *Fraction-free algorithms for linear and polynomial equations*," Tech Report, NAWCADPAX, 1997.

This report extends the ideas behind Bareiss's fraction-free Gauss elimination algorithm in a number of directions. First, in the realm of linear algebra, algorithms are presented for fraction-free LU "factorization" of a matrix and for fraction-free forward and backward substitution. These algorithms are valid not just for integer computation, but also for any matrix system where the entries are taken from a unique factorization domain such as a polynomial ring. The second part of the paper applies a fraction-free formulation to resultant algorithms for solving polynomial systems. In particular, the use of fraction-free polynomial arithmetic and triangularization algorithms in computing the Dixon resultant of a polynomial system is discussed in detail.

Presentations

BAKER, Mitchell, Professor, "A Dynamical Systems Approach to Cardiac Arrhythmias", AMS Sectional Meeting/*Univ. of Louisiana at Lafayette*, April 21, 2000.

BAKER, Mitchell, Professor, "Product States and the AT Property for the Guage Invariant and Rotation Invariant CAR Algebras," Great Plains Operator Theory Symposium, University of San Juan, San Juan, Puerto Rico, May 27, 2000.

BOLLT, Erik M., Associate Professor, Chaos Brown Bag Lunch, U. of Maryland, MD, "On the Inverse Frobenius-Perron Problem: Control of Chaos by Stabilization of Invariant Measures," April 27, 2000.

BOLLT, Erik M., Associate Professor, Invited Colloquium Lecture, George Washington University, "On the Inverse Frobenius-Perron Problem: Global Stabilization of Arbitrary Invariant Measures," November 19, 1999.

BOLLT, Erik M., Associate Professor, Invited Student Lecture, University of Denver, "Chaos, Control: Opposite Sides of the Same Coin," October 22, 1999.

BOLLT, Erik M., Associate Professor, "Model Selection, Confidence, and Scaling in Predicting Chaotic Time-Series," 5th Experimental Chaos Conference, June 28-July 1, 1999.

BOLLT, Erik M., Associate Professor, "Model Selection, Confidence, and Scaling in Predicting Chaotic Time-Series," and "Dynamics of coding in communicating with chaos," and "Optimal Targeting," and "On the Inverse Frobenius-Perron Problem: Global Stabilization of Arbitrary Invariant Measures," at the SIAM Dynamical Systems Conference, Snowbird, UT, May, 1999.

BOLLT, Erik M., Associate Professor, "A Solution to the Inverse Frobenius-Perron Problem, "IEEE ISCAS'00 Circuit and Systems Society meeting, Geneva, Switzerland, May 27, 2000.

CRAWFORD, Carol G., Professor, *Chair, Officers and Business Meetings,* MD-DC-VA Fall Section Conference, Loyola College, Baltimore, MD, 12-13 November 1999.

CRAWFORD, Carol G., Professor, with MEYERSON, Mark D., Professor, *"Interactive Web Based Labs for the U.S. Naval Academy - Real World Applications Designed with Java for the 3-semester Calculus Sequence"*, National Meeting of The Mathematical Association of America, Washington, DC , 20 January 2000.

CRAWFORD, Carol G., Professor, *Chair, Officers and Business Meetings,* MD-DC-VA Spring Section Conference, Bowie State University, 28-29 April 2000.

FOWLER, Gary O., Associate Professor, "The advantage of teaching prediction intervals." Sixth International Conference of Statistics, Combinatorics and Related Areas, December 1999.

GAGLIONE, Anthony M., Professor, "The wreath product ZwrZ is not discriminating." NY Group Theory Seminar, CUNY Graduate Center, New York, NY, 8 Oct 1999.

GAGLIONE, Anthony M., Professor, "What is the probability that two elements of a groups commute?" Fairfield University, Fairfield CT, 12 Nov 1999.

GAGLIONE, Anthony M., Professor, "The TI-92 in the Teaching of Calculus," AMS-MAA National Meeting, Washington DC, 22 Jan 00.

GAGLIONE, Anthony M., Professor, "The finitely generated free nil-2 groups are not discriminating," NY Group Theory Seminar, CUNY Graduate Center, New York, NY 29 Apr 2000.

GAGLIONE, Anthony M., Professor, "Are some groups less discriminating than others, I" Ohio-Denison Group Theory Conference, held at Ohio State Univ, Columbus OH, 21 May 1999.

GAGLIONE, Anthony M., Professor, "Are Some Groups Less Discriminating Than Others," National meetings of the Canadian Math Society, Math 2000, McMaster Univ., Hamalton, Ontario, Canada, 12 Jun 2000.

GARCIA, Sonia, M., Associate Professor, "Modeling and Simulation in the Navy," Naval Post-Graduate School, 18 Oct 1999.

GARCIA, Sonia, M., Associate Professor, "Modeling and Simulation in the Navy," TEAMS - Naval Warfare Surface Center, Dahlgren, VA, 24 Sep 1999.

HOFFMAN, Michael, Professor, "Algebraic Structures on the Set of Multiple Zeta Values," session on Interaction of Physics, Number Theory and Computer Science, 5th Annual IMACS Conference on Applications of Computer Algebra, Madrid Spain, 27 Jun 1999.

HOFFMAN, Michael, Professor, "Multiple Zeta Values: New Applications and Identities," Mathematics Colloquium, USNA, 1 Sep 1999.

HOFFMAN, Michael, Professor, "Values of Derivative Polynomials and Counting Snakes," Howard University Combinatorics Seminar, 16 Nov 1999.

HOFFMAN, Michael, Professor, "Noncommutative Derivations and Multiple Zeta Values," Mid-Atlantic Algebra Conference, Fairfax, VA, 12 Mar 2000.

HOFFMAN, Michael, Professor, "Multiple Zeta Values, Quasi-Symmetric Functions, and Mirror Symmetry," Lehigh Geometry/ Topology Conference, Bethlehem, PA, 11 Jun 2000.

JOYNER, David, Professor, "Goppa Codes for Varieties," U.S. Naval Academy, Annapolis, MD August 1999.

JOYNER, David, Professor, "Multiplicity one for SL(2)," Yale University, 30 Mar 2000.

KAPLAN, Harold M., Professor, "The Mean of a Bounded Finite Population," Mid-Atlantic Probability and Statistics Day, University of Maryland, Baltimore, MD, 13 Nov 1999.

KIDWELL, Mark, Professor, "Solution to a conjecture of Stoimenow about plane curves," Knots mini-conference IX, 24 Sep 1999.

KONKOWSKI, Deborah A., Professor, "Testing a Stability Conjecture for Plane Wave Cauchy Horizons," Contributed Talk at 9th Midwest Geometry Conference, University of Missouri - Columbia, Missouri, November 1999.

KONKOWSKI, Deborah A., Professor, "Testing a Stability Conjecture for Plane Wave Cauchy Horizons," Talk at 9th Midwest Relativity Meeting, University of Illinois at Urbana/Champaign, Illinois, November 1999.

KONKOWSKI, Deborah A., Professor, "Quantum Singularity of Quasiregular Spacetime - Waves on Tod Spacetime," Talk at 4th Eastern Gravity Meeting, Dubquesne University, Pittsburgh, PA, April 2000.

KONKOWSKI, Deborah A., Professor, "Nature and Stability of Tod Spacetime," Contributed Talk at American Physical Society April 2000 Meeting, Long Beach, CA, April 29-May 2, 2000.

KONKOWSKI, Deborah A., Professor, "Quantum Singularity of Quasiregular Spacetime," London Relativity Seminar, Queen Mary & Westfield College, London, U.K., 7 Jun 2000.

MARUSZEWSKI, Richard F., Professor, "The Structure of Natural Languages," Mathematics Department Cryptology Seminar.

MCCOY, Peter A., Professor, "On the Radiating Solutions to the Helmholtz Equation and Inverse Scattering," Session on Partial Differential Equations, American Mathematical Society Annual Meeting, Washington DC, 21 Jan 2000.

MCCOY, Peter A., Professor, "Electromagnetic Scattering in Three Dimensions," Special Session Honoring G.G. Walter, IMACS 2000, University of Wisconsin, Milwaukee, 24 May 2000.

MELLES, Caroline Grant, Associate Professor, "Complete Kahler Metrics for Singular Toroidal Varieties," AMS Special Session, Joint Mathematics Meetings, Washington DC, 19 Jan 2000.

MEYERSON, Mark D., Professor, "Electronic Syllabus" and "Web Based Math Labs," to United States Naval Academy, September 1999.

MEYERSON, Mark D., Professor, "Real World Calculus Laboratory - Interactive Web Based Labs Designed with Java," American Mathematical Society Annual Meeting, Washington DC, 21 Jan 2000.

MICHAEL, T.S., Associate Professor, "Two New Art Gallery Theorems," Combinatorics Conference, Kalamazoo, Michigan, June 2000.

MICHAEL, T.S., Associate Professor, "Rigidity and Rank at Annapolis: Hadamard Matrices," University of Pennsylvania Combinatorics Seminar, April 2000.

MICHAEL, T.S., Associate Professor, "Hadamard Matrices," The George Washington University, Mathematics Department Colloquium, October 1999.

MICHAEL, T.S., Associate Professor, "Prison-Yards, Art Galleries, and Embedding," United States Naval Academy, Mathematics Department Colloquium, August 1999.

NAKOS, George, Professor and Williams, Robert, "Triangularization of Polynomial Systems with the Dixon Resultant," IMACS International Conference, Athens, Greece, July 1999.

STANFORD, Theodore, Assistant Professor, "Knots and Links Modulo Braid Subgroups," 9th biannual mini-conference at George Washington University, 25 Sep 1999.

STANFORD, Theodore, Assistant Professor, "Braid Commutators and Vassiliev's Knot Invariants," Mathematics Department Colloquium, University of Oregon, 28 Jan 2000.

STANFORD, Theodore, Assistant Professor, "Undoing Knots and Undoing Other Things," Mathematics Department Colloquium, New Mexico State University, 4 Apr 2000.

TRAVES, William N., Assistant Professor, "Differential Simplicity and Tight Closure," Midwest Algebraic Geometry Conference, University of Missouri at Columbia, October 1999.

TRAVES, William N., Assistant Professor, "Cliques at the Naval Academy," Regional MAA Meeting, Loyola College, November 1999.

TRAVES, William N., Assistant Professor, "Differential Simplicity," Mid-Atlantic Algebra Conference, George Mason University, March 2000.

TRAVES, William N., Assistant Professor, "Fair Cake Cutting after Su," Regional MAA Meeting, Bowie State University, April 2000.

TRAVES, William N., Assistant Professor, "Differential Operators on Toric Varieties," AMS-IMS-SIAM Research Conference, Mount Holyoke University, June 2000.

TURNER, John C., Professor, "Confidence Interval Using Probability," University of Colorado, Denver, CO, March 2000.

TURNER, John C., Professor, "Spreadsheet Solution for Fisher's Exact Test," Western Statistics Teachers Conference, Greely, CO, March 2000.

TURNER, Peter R., Professor, "The Symmetric Level-Index System with an Application to Chaos," invited paper to appear in the Proceedings of CSCC2000, Athens, Greece, July 2000.

TURNER, Peter R., Professor, "Image and Moving Object Identification in Computer ision," ICIAM99, Edinburgh, Scotland, July 1999.

TURNER, Peter R., Professor, NAKOS, G., Professor, and Williams, R.M., "Fraction-free Algorithms for Linear and Polynomial Equations," ECCAD, East Coast Computer Algebra Days, Boston, MA, May 1997.

TURNER, Peter R., Professor, "Fraction-free RNS Algorithms for Solving Linear Systems," ARITH13, Asilomar, CA, July 1997.

TURNER, Peter R., Professor, "Fraction-free RNS Algorithms for Solving Linear Systems," SIAM National Meeting, Stanford, CA, July 1997.

WARDLAW, William P., Professor, invited presentation (5 hours): "Crypto Workshop," at spring meeting of Indiana Section of MAA at Earlham College in Richmond, IN, on 7-8 April 2000.

WARDLAW, William P., Professor, "An Elementary School Approach to the 16 Puzzle," spring meeting of the MD-VA-DC Section of the MAA, Bowie State University, Bowie, MD, on 29 April 2000.