AD-A243 163

DTIC
S ELECTE DEC 1 0 1991 D
C

UNBD
1

May 1991

M91-40

R. A. Games

FY92 Mathematical Research Project Proposal Briefing

Approved for public release;
distribution unlimited.

MITRE
Bedford, Massachusetts

91 1209 117

91-17465

May 1991

M91-40

R. A. Games

FY92 Mathematical Research Project Proposal Briefing

Accession For
NTIS GRA&I
DTIC TAB
Unannounced
Justification
By
Distribution/
Availability Codes
Dist | Avail and/or Special
A-1

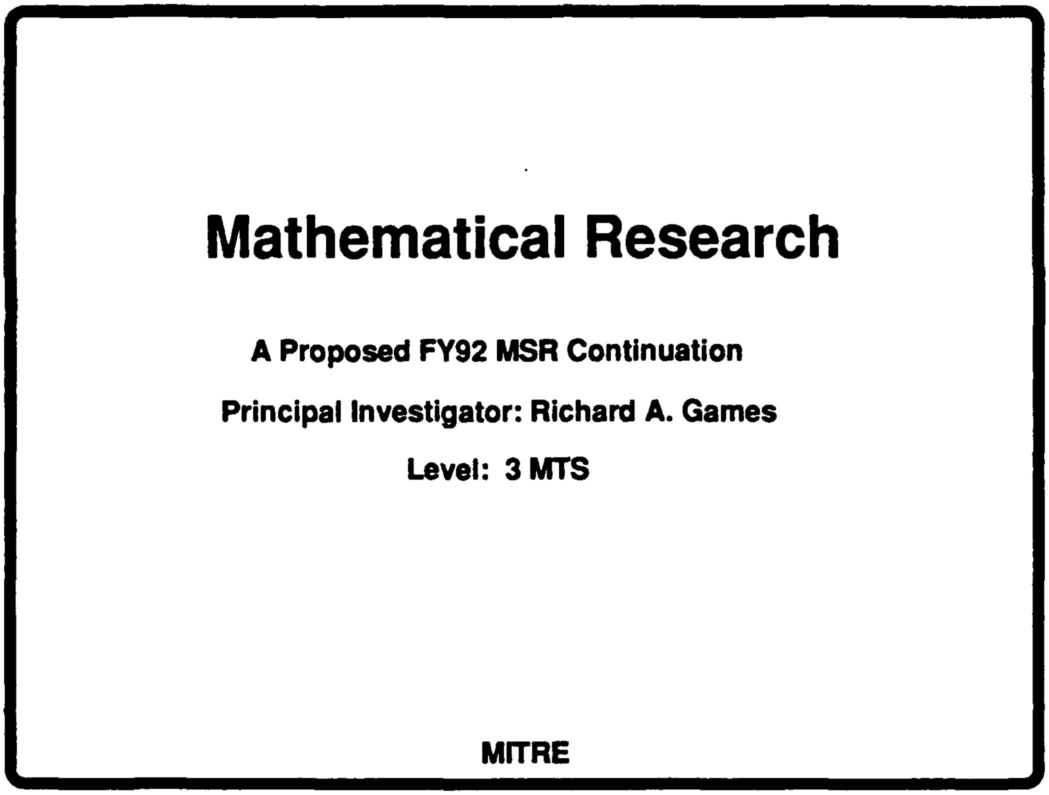
CONTRACT SPONSOR MSR
CONTRACT NO. N A
PROJECT NO. 9025X
DEPT. D082

Approved for public release;
distribution unlimited.

MITRE

The MITRE Corporation
Bedford, Massachusetts

Annotations for FY92 Mathematical Research Project Proposal Briefing
Delivered 10 April 1991



Mathematical Research

A Proposed FY92 MSR Continuation

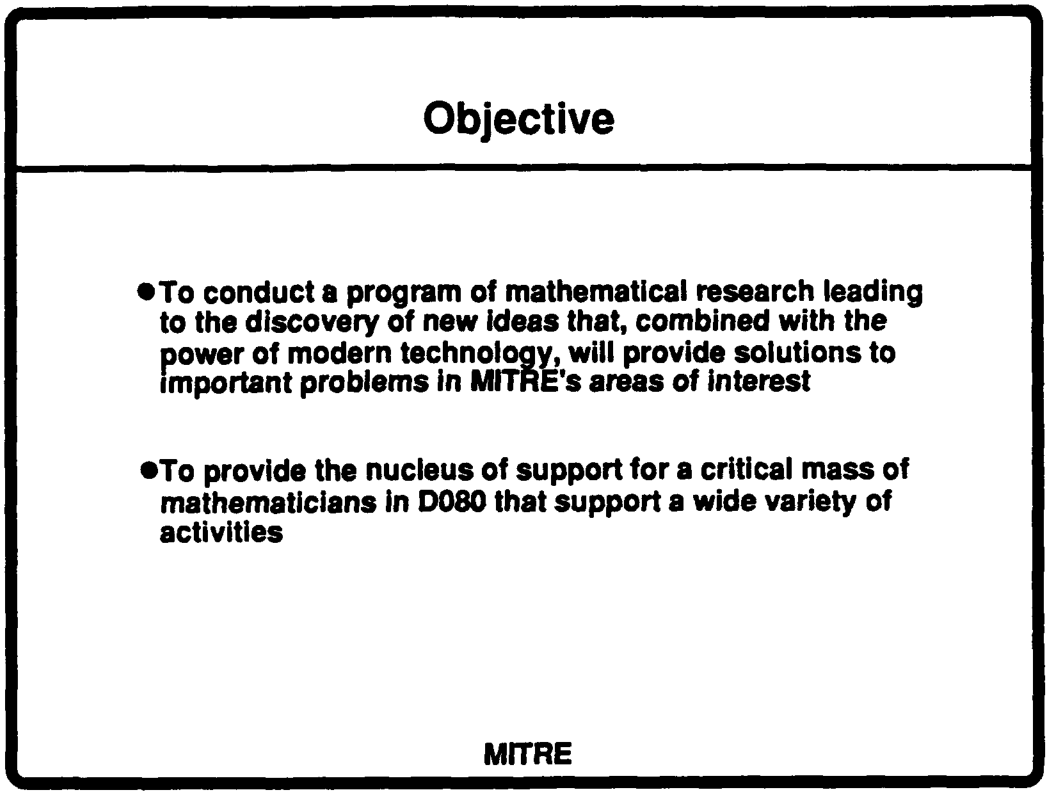
Principal Investigator: Richard A. Games

Level: 3 MTS

MITRE

Title Slide: Mathematical Research

Many areas in mathematics are directly applicable to MITRE's work program. Coding theory and pseudorandom sequences are important in resolving security issues. Graph theory is an indispensable tool in the design of very large scale integrated circuits and the analysis of parallel algorithms. The use of ideas from such diverse fields as number theory and harmonic analysis is commonplace in modern signal processing. Stochastic processes play a key role in communication theory. The Mathematical Research project was established in 1982 in response to the growing need for mathematical sophistication within the corporation's work program. Project personnel support this need by conducting research in relevant areas of mathematics and by working directly with other projects in MITRE's work program.



Objective

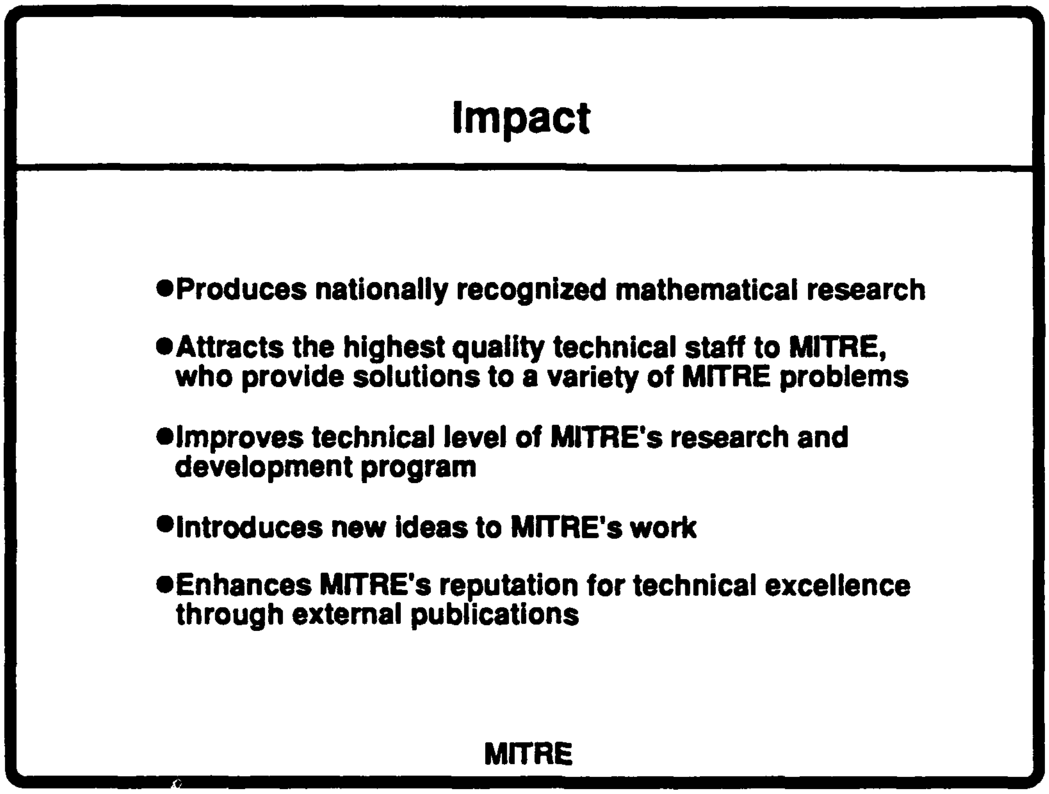
- To conduct a program of mathematical research leading to the discovery of new ideas that, combined with the power of modern technology, will provide solutions to important problems in MITRE's areas of interest

- To provide the nucleus of support for a critical mass of mathematicians in D080 that support a wide variety of activities

MITRE

Objective

This project represents a continuing commitment to a program of mathematical research at MITRE. The aim is to develop new ideas that, when combined with modern technology, provide solutions to important problems in command, control, communications, and intelligence systems. A further objective is to maintain the mathematical expertise necessary to promote the use of rigorous methods throughout MITRE's work program. Organizing this capability within one project fosters the development of complementary skills and encourages collaboration between project members.



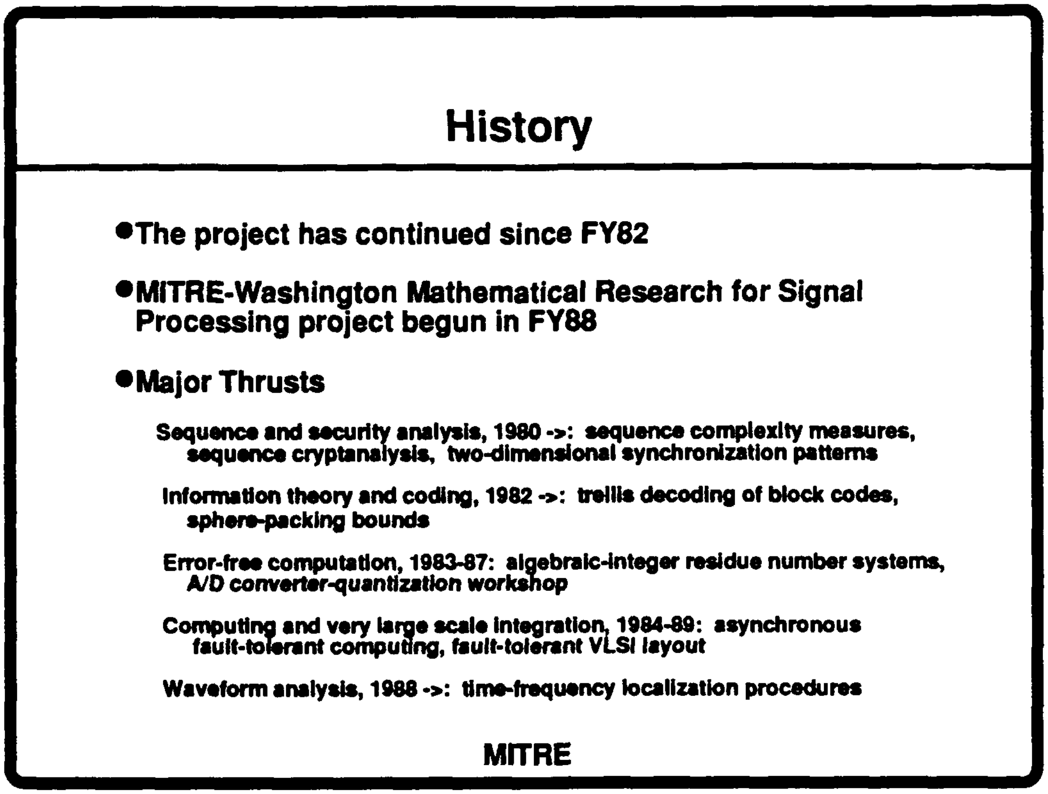
Impact

- Produces nationally recognized mathematical research
- Attracts the highest quality technical staff to MITRE, who provide solutions to a variety of MITRE problems
- Improves technical level of MITRE's research and development program
- Introduces new ideas to MITRE's work
- Enhances MITRE's reputation for technical excellence through external publications

MITRE

Impact

Next year will be the ten-year anniversary of the project. Over the last decade the project has significantly impacted MITRE's work, particulary within D080. Over the next decade we will continue to broaden our impact on other parts of MITRE, initiating interactions in those areas where we feel there is the potential for the application of mathematics. In addition to their mathematical research, members of the project work closely with MITRE engineers to strengthen the theoretical basis of the system acquisition and planning programs or other technology projects. This project enhances MITRE's prominence in the information technology disciplines through its publications and interactions with other research and development organizations.



History

- The project has continued since FY82
- MITRE-Washington Mathematical Research for Signal Processing project begun in FY88
- Major Thrusts

Sequence and security analysis, 1980 ->: sequence complexity measures, sequence cryptanalysis, two-dimensional synchronization patterns

Information theory and coding, 1982 ->: trellis decoding of block codes, sphere-packing bounds

Error-free computation, 1983-87: algebraic-integer residue number systems, A/D converter-quantization workshop

Computing and very large scale integration, 1984-89: asynchronous fault-tolerant computing, fault-tolerant VLSI layout

Waveform analysis, 1988 ->: time-frequency localization procedures

MITRE

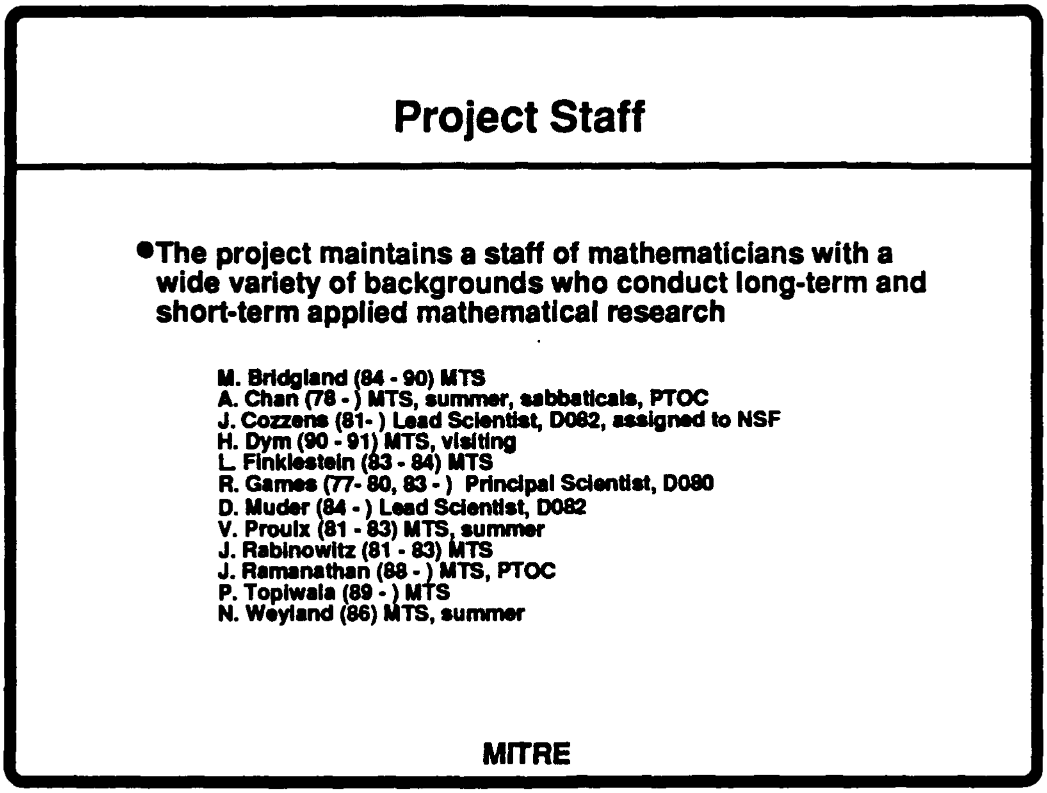
History

Our initial work areas were pseudorandom sequences and error-correcting codes. We have supported long-term efforts in these areas and have made significant contributions. We have introduced new techniques for constructing pseudorandom sequences and have established bounds on the complexity of these sequences. We have developed new constructions for two-dimensional synchronization patterns used for ranging. We have analyzed various techniques for decoding error-correcting codes and have made new contributions to trellis decoding of block codes and to trellis-coded modulation. In recent years, we have taken a more theoretical look at the problem of error correction, which has motivated our interest in sphere packing. We have obtained improved bounds on the density of optimal packings and new characterizations of their local structure.

In 1983, we began to examine techniques for error-free computation, particularly integer processing with residue number systems. We developed a novel method for quantizing real and complex data by using dense rings of algebraic integers, and we showed how this could be combined with residue number system processing to compute an error-free discrete Fourier transform. This work continued for several years and was eventually transferred to the Algebraic Integer Quantization and Conversion project in 1987.

We became interested in the application of graph-theoretic techniques to signal processing. We solved graph-theoretical problems concerning the very large scale integrated (VLSI) layout of a fault tolerant configuration of processors. Our work in this area also produced a generalization of a central theorem about asynchronous distributed algorithms.

More recently, we have also studied joint time-frequency and time-scale representations of signals. We have proved a theorem characterizing certain nonstationary random processes by properties of their time-scale transforms and are developing improved time-frequency localization techniques for detection and noise-reduction applications involving signals with time-varying frequency content.



Project Staff

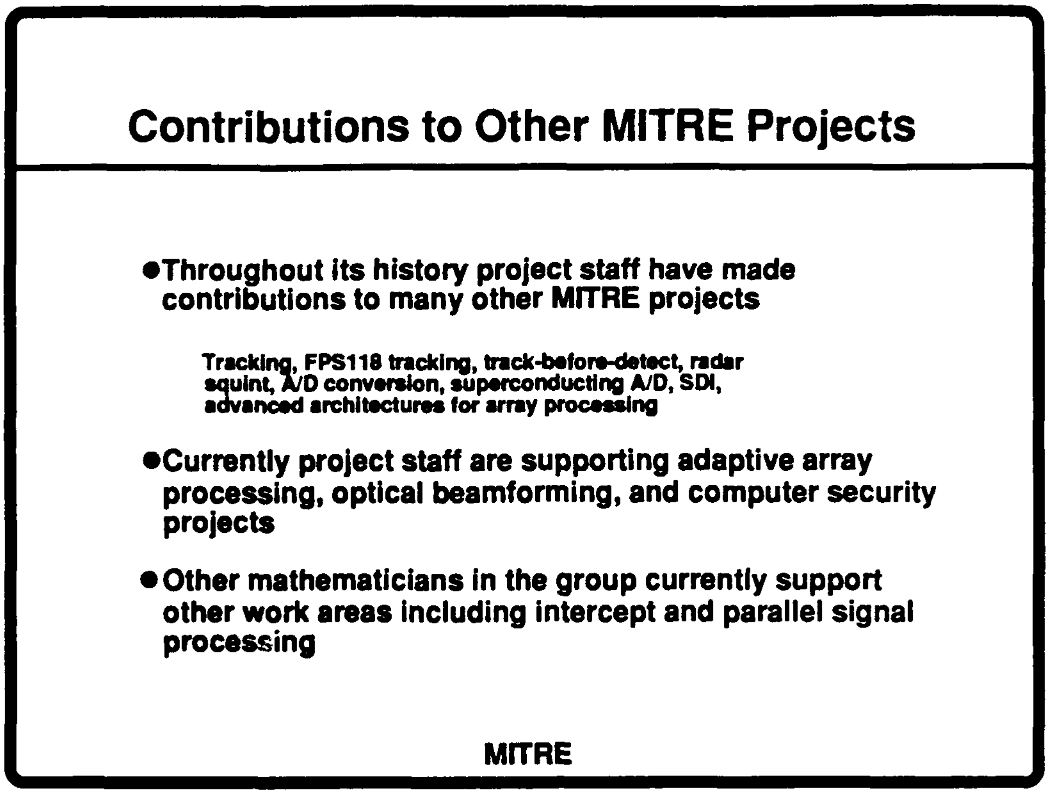
- The project maintains a staff of mathematicians with a wide variety of backgrounds who conduct long-term and short-term applied mathematical research

M. Bridgland (84 - 90) MTS
A. Chan (78 -) MTS, summer, sabbaticals, PTOC
J. Cozzens (81-) Lead Scientist, D082, assigned to NSF
H. Dym (90 - 91) MTS, visiting
L Finklestein (83 - 84) MTS
R. Games (77- 80, 83 -) Principal Scientist, D080
D. Muder (84 -) Lead Scientist, D082
V. Proulx (81 - 83) MTS, summer
J. Rabinowitz (81 - 83) MTS
J. Ramanathan (88 -) MTS, PTOC
P. Topiwala (89 -) MTS
N. Weyland (86) MTS, summer

MITRE

Project Staff

Over the years the project has supported a number of high-quality research mathematicians, including two Lead Scientists in D082 and a Principal Scientist in D080. John Cozzens, a charter member of the project, is currently on leave to the National Science Foundation where he directs the Circuits and Signal Processing work area. Harry Dym, an internationally known mathematician, visited in FY91.



Contributions to Other MITRE Projects

- Throughout its history project staff have made contributions to many other MITRE projects

  Tracking, FPS118 tracking, track-before-detect, radar squint, A/D conversion, superconducting A/D, SDI, advanced architectures for array processing

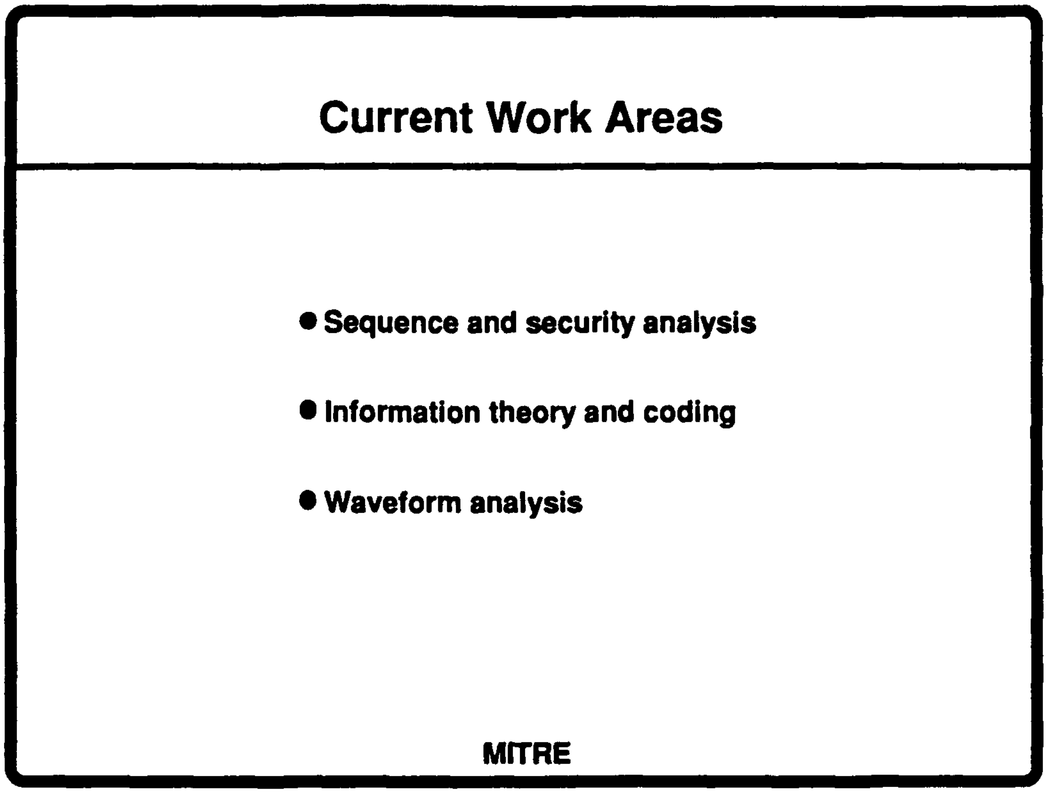
- Currently project staff are supporting adaptive array processing, optical beamforming, and computer security projects

- Other mathematicians in the group currently support other work areas including intercept and parallel signal processing

MITRE

Contributions to Other MITRE Projects

Members of the project maintain an awareness of current developments in mathematics and its applications and initiate the assimilation of new mathematical discoveries into MITRE's work program. Project personnel work in conjunction with other MITRE projects to address more immediate problems requiring mathematical analysis. Recent examples of such contributions include work on covert channels in secure computer systems, analog-to-digital conversion, tracking, and adaptive signal processing. These collaborations also help us to identify areas of mathematics that are potentially applicable to MITRE's future work and to select important research problems in these areas.



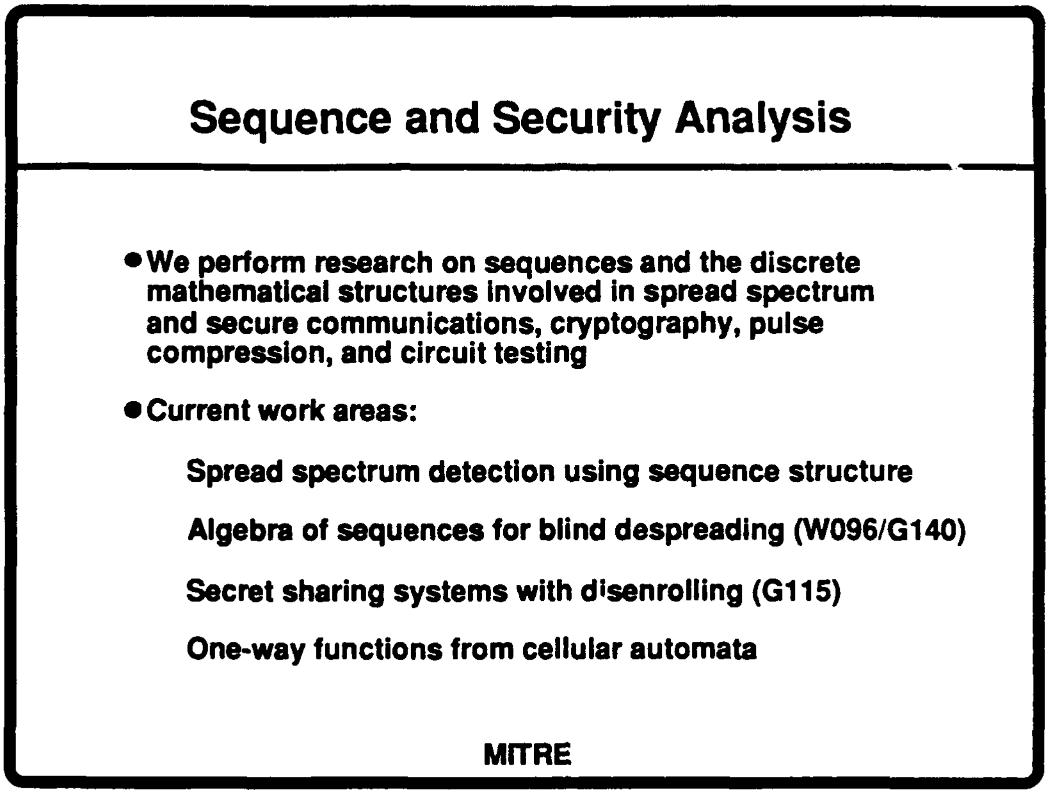
Current Work Areas

- Sequence and security analysis
- Information theory and coding
- Waveform analysis

MITRE

Current Work Areas

Members of the project conduct a concerted program of mathematical research and analysis on problems whose solutions are required for overcoming performance limitations of current and future command, control, and communications systems. We have ongoing mathematical research programs in the following general areas: sequence and security analysis, information theory and coding, and waveform analysis.



Sequence and Security Analysis

- We perform research on sequences and the discrete mathematical structures involved in spread spectrum and secure communications, cryptography, pulse compression, and circuit testing
- Current work areas:

  Spread spectrum detection using sequence structure

  Algebra of sequences for blind despreading (W096/G140)

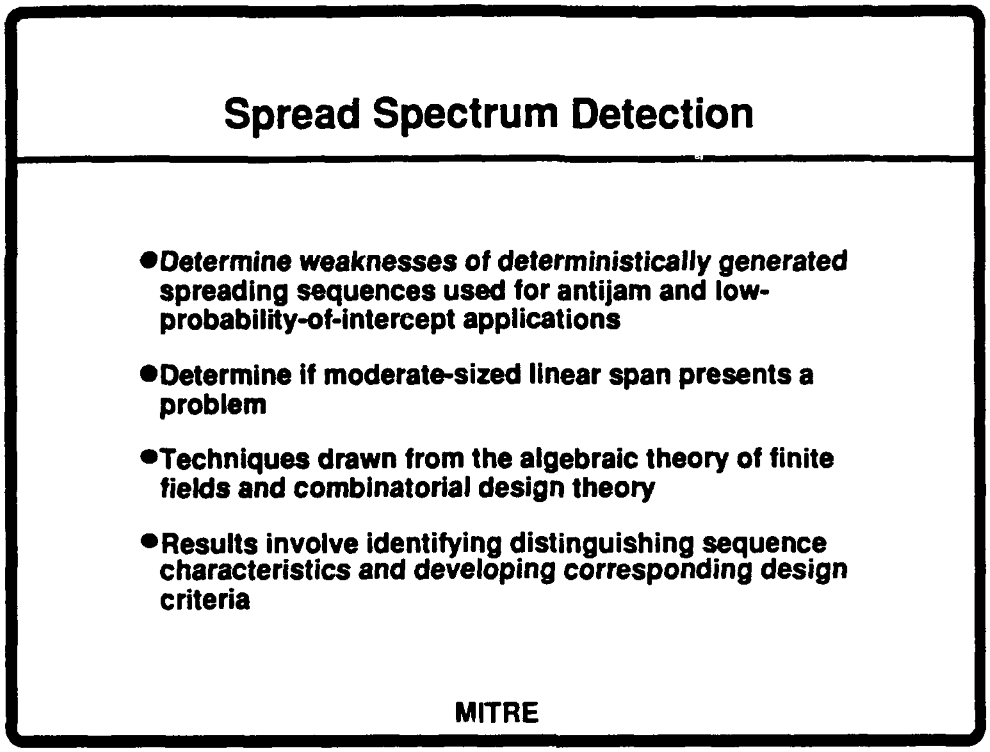
  Secret sharing systems with disenrolling (G115)

  One-way functions from cellular automata

MITRE

Sequence and Security Analysis

We perform research on sequences and the discrete mathematical structures involved in a variety of command, control, communication, and intelligence applications. Randomly generated sequences play an important role in a variety of applications, including secure communications, spread spectrum communications, radar signal design, sonar, and the testing of complicated integrated circuits. Although random sequences are desirable, most practical systems use deterministically generated sequences that pass certain statistical randomness tests. Our ongoing research in this area analyzes the complexity and correlation properties of these so-called pseudorandom sequences in the context of a variety of applications.



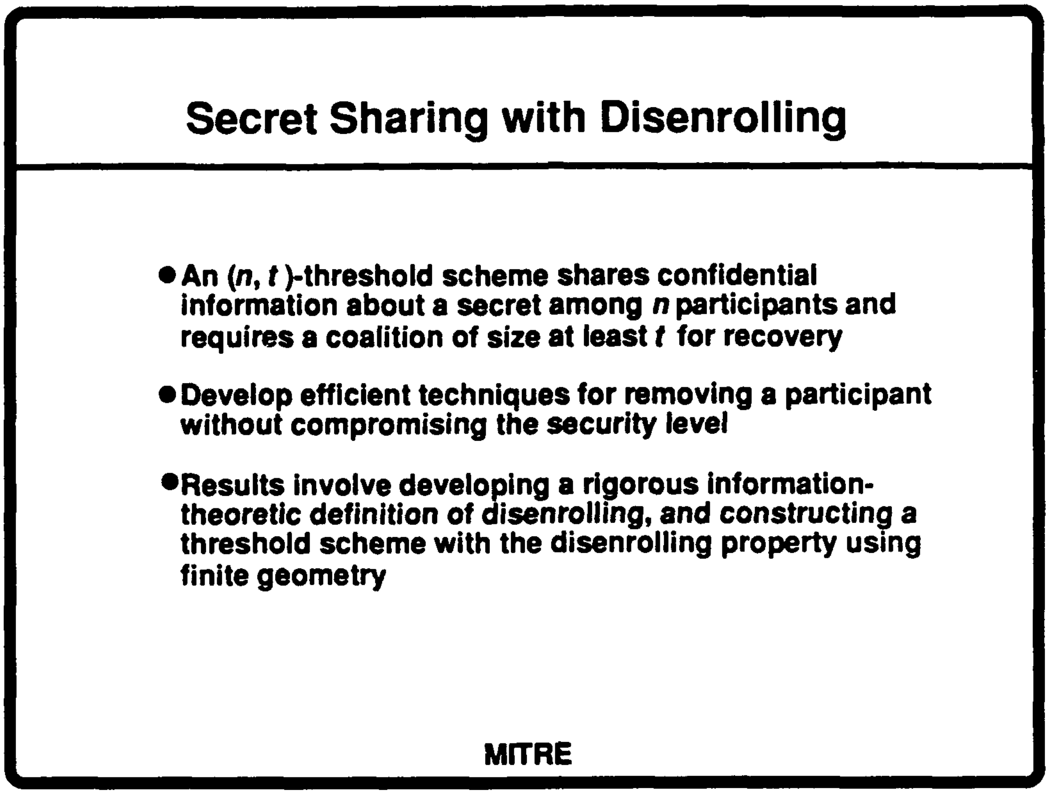
Spread Spectrum Detection

- Determine weaknesses of deterministically generated spreading sequences used for antijam and low-probability-of-intercept applications
- Determine if moderate-sized linear span presents a problem
- Techniques drawn from the algebraic theory of finite fields and combinatorial design theory
- Results involve identifying distinguishing sequence characteristics and developing corresponding design criteria

MITRE

Spread Spectrum Detection

Direct-sequence spread spectrum systems, like MITRE's wide-bandwidth high-frequency communications system, use deterministically generated sequences to encode the transmitted data. We have been considering questions of whether the structure contained in these spreading sequences makes it easy to detect the transmission when low-probability-of-intercept communications are desired. We have initially focused on the linear feedback shift register sequences that are used in the MITRE communications facility, deriving guidelines for choosing the most appropriate generator for covert communications. Surprisingly, our criterion is equivalent to the one derived by James H. Lindholm in the 1960s when he was selecting generators with the most suitable partial-period correlation properties. We will continue this avenue of research to develop improved detection attacks based on more subtle properties of the spreading sequences. We are also collaborating with MITRE Washington (W096/G115) on the problem of blind despreading, or actually determining the spreading sequence, again by relying on the algebraic structure underlying these sequences. The potential importance of this subject grows, since code-division multiple-access systems are being considered for cellular communication and wireless local-area networks.



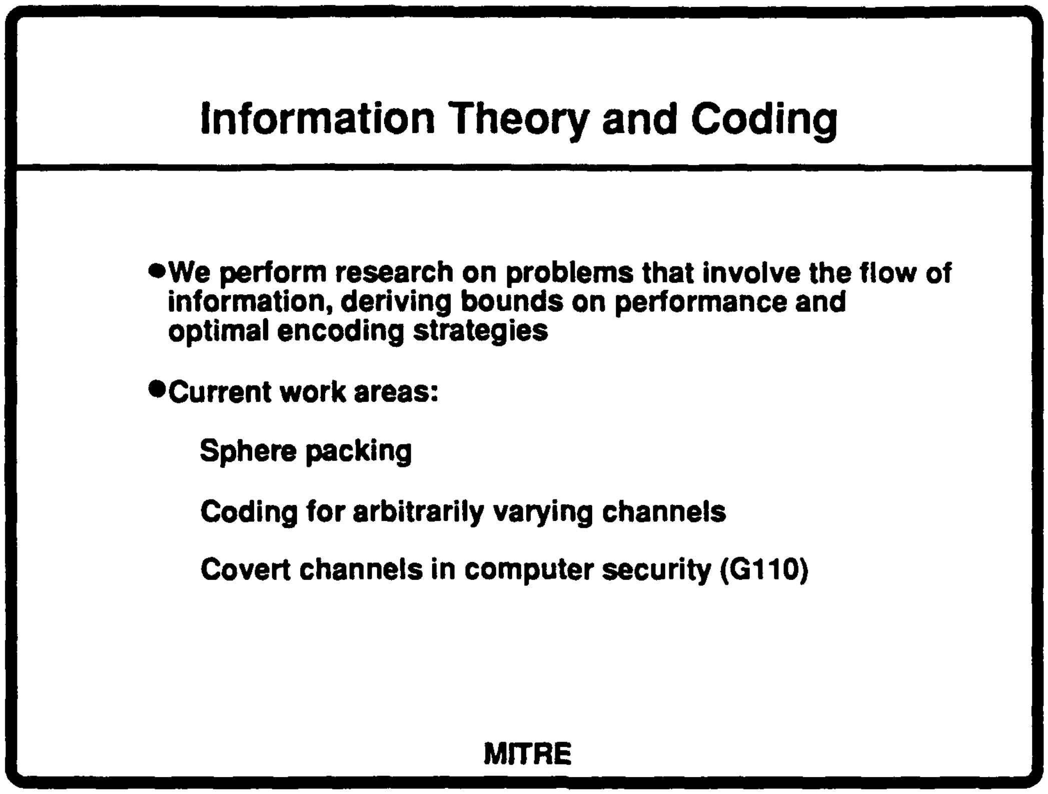
Secret Sharing with Disenrolling

- An (*n*, *t*)-threshold scheme shares confidential information about a secret among *n* participants and requires a coalition of size at least *t* for recovery
- Develop efficient techniques for removing a participant without compromising the security level
- Results involve developing a rigorous information-theoretic definition of disenrolling, and constructing a threshold scheme with the disenrolling property using finite geometry

MITRE

Secret Sharing with Disenrolling

In many applications it is desirable to distribute the ability to initiate an important action. One approach is to form what is called an (n, t)-threshold scheme, where secret shares are distributed to n participants with the property that a secret key can be recovered if at least t of the participants combine their confidential information. These schemes have built-in redundancy when $n > t$ that allows participants to drop out without affecting the group's ability to act. The problem we have been considering is how to remove a participant while still maintaining the same security level (t). If the share of the removed person is published, the security level of the scheme drops to $t - 1$. In conjunction with researchers at Texas A & M University, we are developing a rigorous information-theoretic definition of disenrolling for this application and are devising threshold schemes based on finite geometries that allow for the efficient recovery of the original security level.



Information Theory and Coding

- We perform research on problems that involve the flow of information, deriving bounds on performance and optimal encoding strategies
- Current work areas:

  Sphere packing

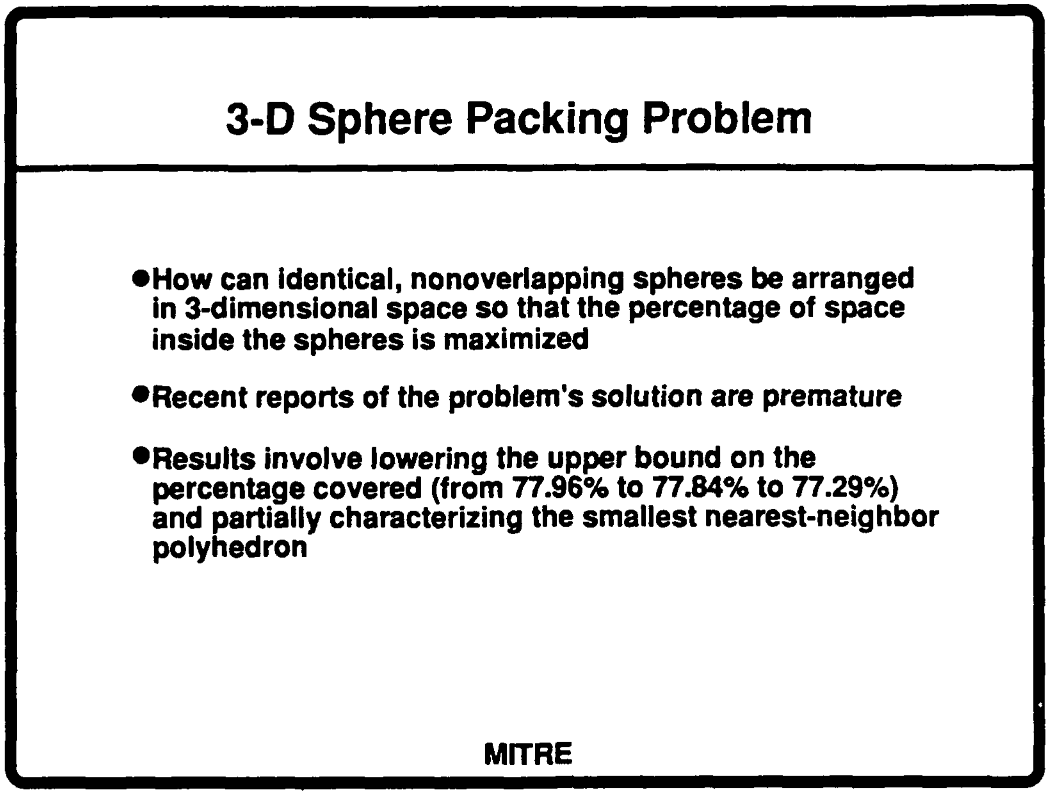
  Coding for arbitrarily varying channels

  Covert channels in computer security (G110)

MITRE

Information Theory and Coding

We perform research on problems that involve the flow of information, deriving bounds on system performance and determining optimal encoding strategies.



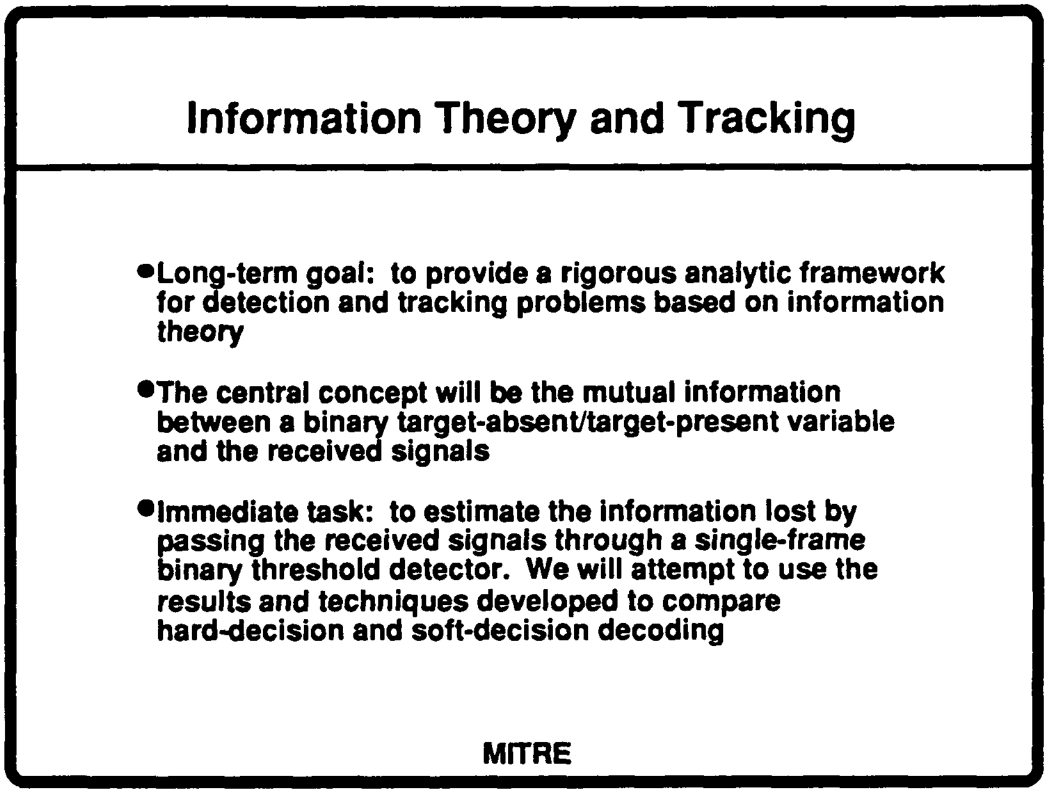
3-D Sphere Packing Problem

- How can identical, nonoverlapping spheres be arranged in 3-dimensional space so that the percentage of space inside the spheres is maximized
- Recent reports of the problem's solution are premature
- Results involve lowering the upper bound on the percentage covered (from 77.96% to 77.84% to 77.29%) and partially characterizing the smallest nearest-neighbor polyhedron

MITRE

3-D Sphere Packing Problem

For a number of years we have done research on sphere packing problems. These problems involve arranging the largest number of identical n-dimensional spheres into a confined region of n-dimensional space in such a way that no two overlap. Such packing problems are common in communications and coding. There are many constructions of good sphere packings, but it is very difficult to prove optimality, even in the case of infinite space, where there are no boundary constraints. Recently Wu-Yi Hsiang, a mathematician at the University of California at Berkeley, has announced a proof that the face-centered cubic lattice (also called the 'the cannonball packing' because cannonballs traditionally were stacked in this pattern) is the optimal sphere packing for three-dimensional space. Because of our previous work on this classic open problem, we have become involved in the verification of Hsiang's proof and have been a source for press reports on this subject. Unfortunately, we have identified holes in the first part of Hsiang's two-step proof and expect to play a major role in the eventual determination of whether or not the three-dimensional problem has in fact been solved.



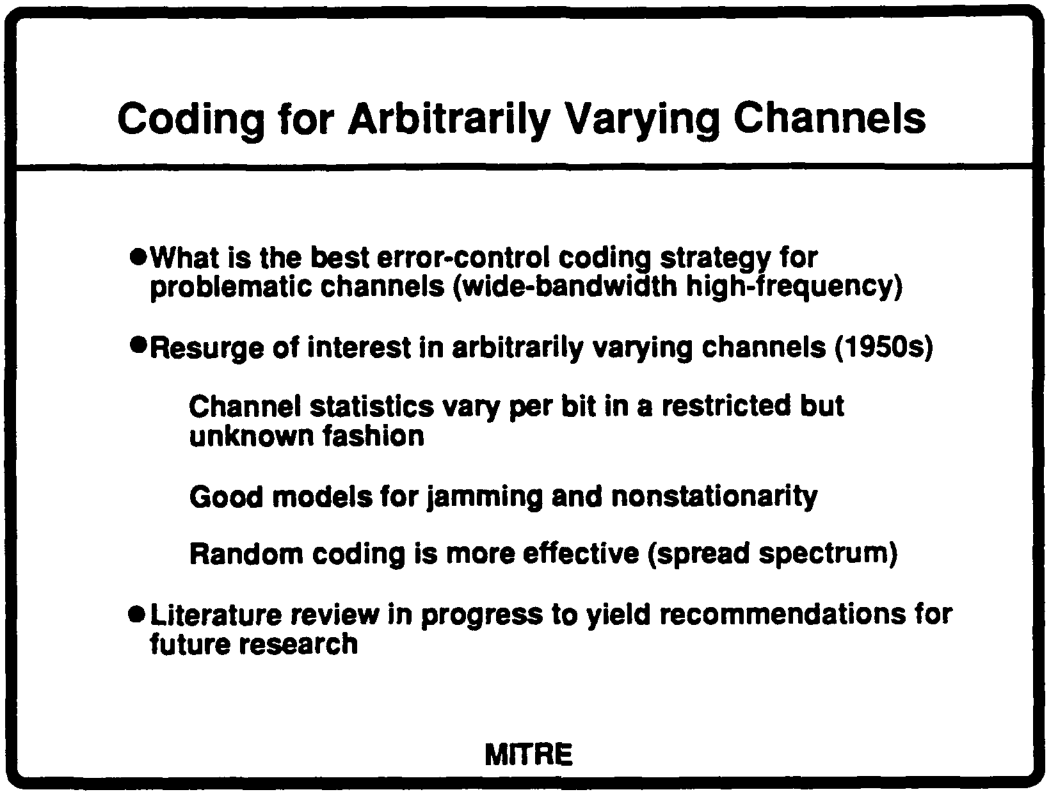
Information Theory and Tracking

- Long-term goal: to provide a rigorous analytic framework for detection and tracking problems based on information theory
- The central concept will be the mutual information between a binary target-absent/target-present variable and the received signals
- Immediate task: to estimate the information lost by passing the received signals through a single-frame binary threshold detector. We will attempt to use the results and techniques developed to compare hard-decision and soft-decision decoding

MITRE

Information Theory and Tracking

In the meantime we plan to consider other applications of information theory. In particular we have identified, through our association with other MITRE work on multitarget tracking, the need for a rigorous analytic framework for assessing the potential of various tracking approaches. We are planning to initiate a research program whose long-term goal will be to provide a rigorous analytic framework for tracking and detection problems based on information theory. The central concept will be the mutual information between a binary target-absent/target-present variable and the received signals. As a first step we plan to estimate the information lost by passing the received signals through a single-frame binary threshold detector. We will attempt to use the results and techniques developed to compare tracking approaches based on hard-decision versus soft-decision trellis methods.



Coding for Arbitrarily Varying Channels

- What is the best error-control coding strategy for problematic channels (wide-bandwidth high-frequency)
- Resurge of interest in arbitrarily varying channels (1950s)

  Channel statistics vary per bit in a restricted but unknown fashion

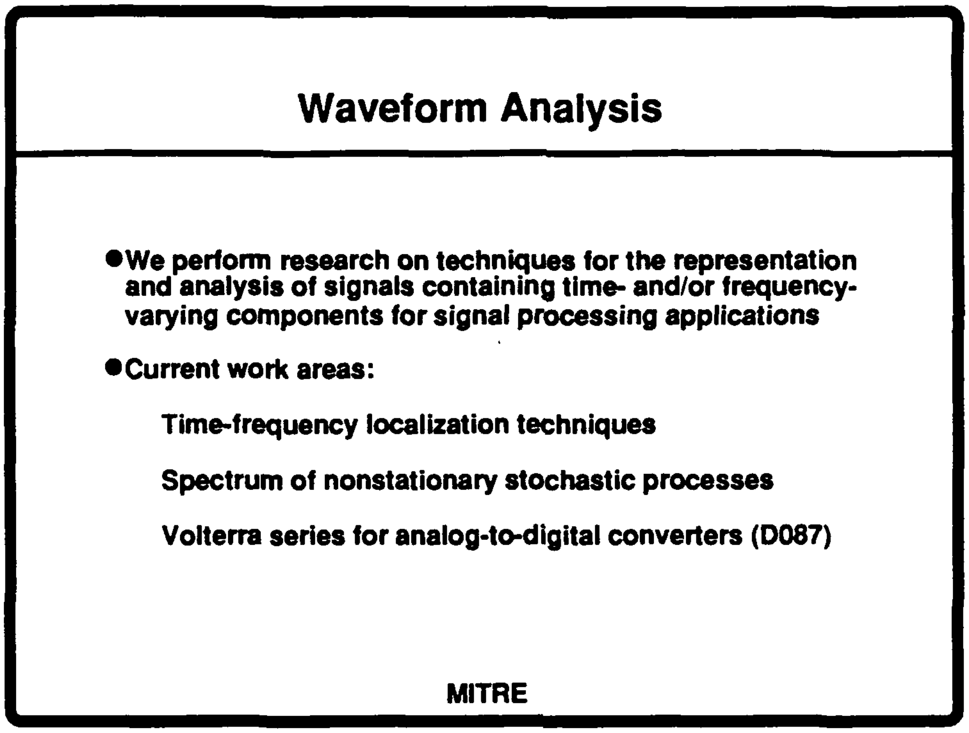
  Good models for jamming and nonstationarity

  Random coding is more effective (spread spectrum)
- Literature review in progress to yield recommendations for future research

MITRE

Coding for Arbitrarily Varying Channels

A problem of considerable current interest to MITRE concerns determining the best error-control coding strategy for a wide-bandwidth high-frequency communication system. The problematic high-frequency (3-30 MHz) channel can be modeled by what has been called an arbitrarily varying channel in which the channel statistics vary per bit in a restricted but unknown fashion. These arbitrarily varying channels have also been used to model the jamming channel, where an adversary varies the channel statistics. There has been a resurgence of interest in this subject, yielding results whose significance needs to be assessed. Future work on this topic will depend on the results of a literature review we are currently conducting.



Waveform Analysis

- We perform research on techniques for the representation and analysis of signals containing time- and/or frequency-varying components for signal processing applications
- Current work areas:

  Time-frequency localization techniques

  Spectrum of nonstationary stochastic processes

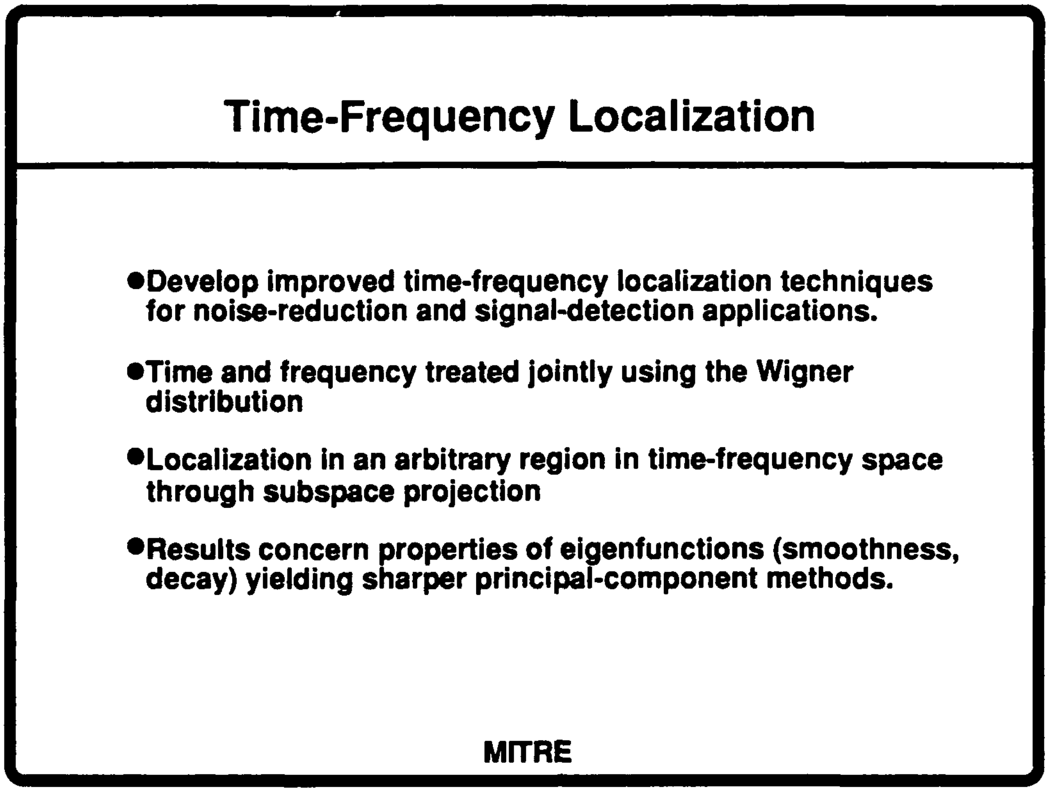
  Volterra series for analog-to-digital converters (D087)

MITRE

Waveform Analysis

We perform research on techniques for the representation and analysis of signals containing time- and frequency-varying components for signal processing applications. Conventional signal processing relies heavily on techniques in Fourier analysis that decompose an arbitrary signal into a superposition of pure tones. A pure tone has frequency characteristics that are constant in time. There are many applications in which signals have frequency characteristics that are time varying or in which the signals are stochastic processes with nonstationary statistics. A traditional time-frequency representation of a signal is computed by correlating the signal with a time and frequency shift of a fixed window. Various techniques of representing the instantaneous frequency content of a signal are under study.

Many systems occurring in science and engineering are analyzed under the assumption that they behave in a linear manner. In reality, practical systems may have nonlinear aspects that are impossible to ignore. We are interested in using Volterra series for the accurate modeling of nonlinear systems, especially with regard to the study of the nonlinearities in high-performance analog-to-digital converters. We plan to continue to focus our efforts on understanding the factors that limit our ability to accurately determine this series representation in practice.



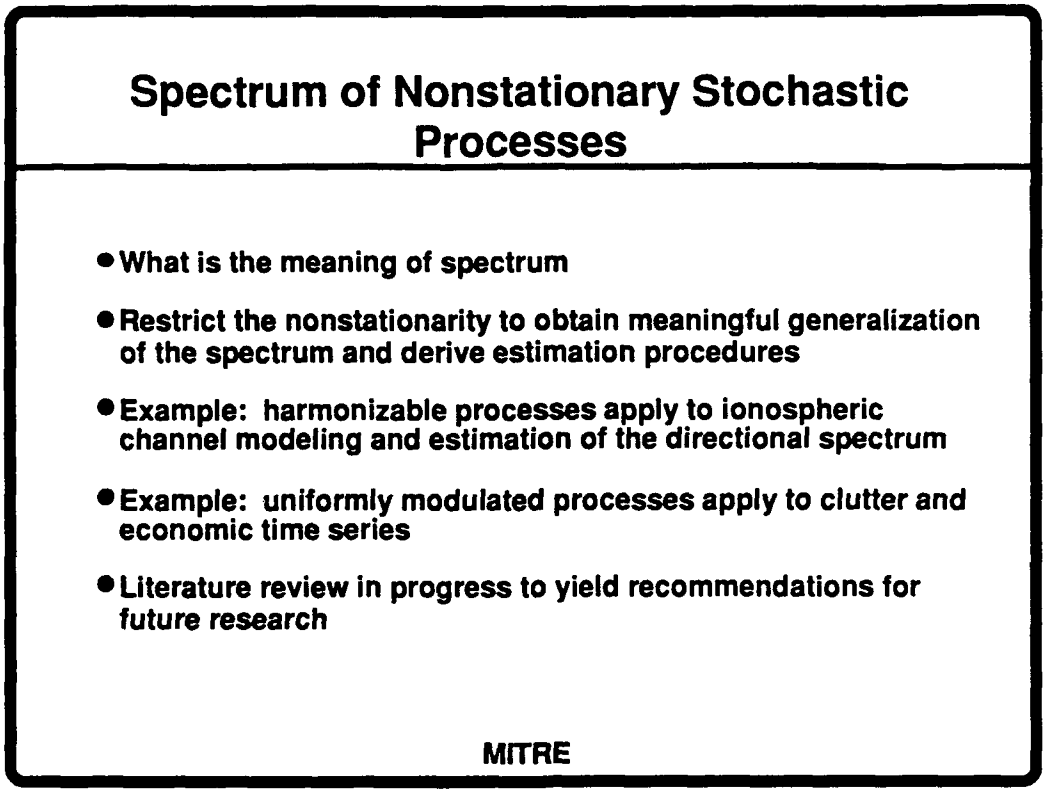
Time-Frequency Localization

- **Develop improved time-frequency localization techniques for noise-reduction and signal-detection applications.**
- **Time and frequency treated jointly using the Wigner distribution**
- **Localization in an arbitrary region in time-frequency space through subspace projection**
- **Results concern properties of eigenfunctions (smoothness, decay) yielding sharper principal-component methods.**

MITRE

Time-Frequency Localization

Recently we have been focusing on time-frequency representations involving the Wigner distribution, which is obtained by taking the Fourier transform of the ambiguity function of a signal. Our objective is to use this representation to obtain improved time-frequency localization techniques. Such techniques can be applied to data to more effectively detect a desired signal with some arbitrary time-frequency characteristic by focusing precisely on the properly shaped regions of time-frequency space, effectively reducing the undesirable effects of other interference and noise. We have obtained results on the projection operators involved that bear on the sharpness of the localization scheme. Empirically our technique appears to improve on the recently published results due to Ingrid Daubechies at ATT Bell Laboratories. We are working to theoretically establish the increase in performance.



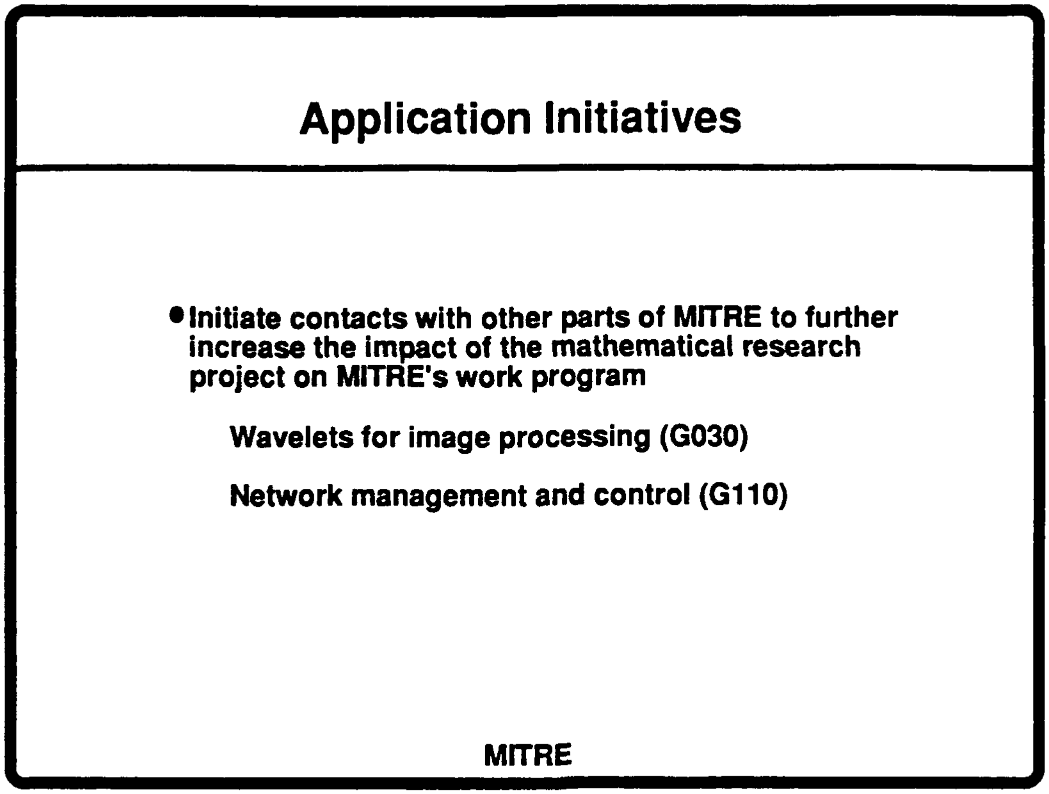
Spectrum of Nonstationary Stochastic Processes

- What is the meaning of spectrum
- Restrict the nonstationarity to obtain meaningful generalization of the spectrum and derive estimation procedures
- Example: harmonizable processes apply to ionospheric channel modeling and estimation of the directional spectrum
- Example: uniformly modulated processes apply to clutter and economic time series
- Literature review in progress to yield recommendations for future research

MITRE

Spectrum of Nonstationary Stochastic Processes

When the signals involved are stochastic processes with time-varying statistics, the usual definition of frequency spectrum is no longer applicable. Often the nonstationarity has to be restricted to allow a meaningful generalization of the spectrum. For example, one model of the nonstationary process produced by the high-frequency ionospheric channel is the process obtained at the output of a time-varying linear filter with a stationary process as its input. The spectrum can be generalized in this case, and provides a useful tool for channel modeling and estimation of the directional spectrum by using antenna arrays. A more rigorous examination of these issues may provide further insight into array performance in the case of the ionospheric channel. We are currently conducting a literature review to assess the potential for future research in this area.



Application Initiatives

- Initiate contacts with other parts of MITRE to further increase the impact of the mathematical research project on MITRE's work program

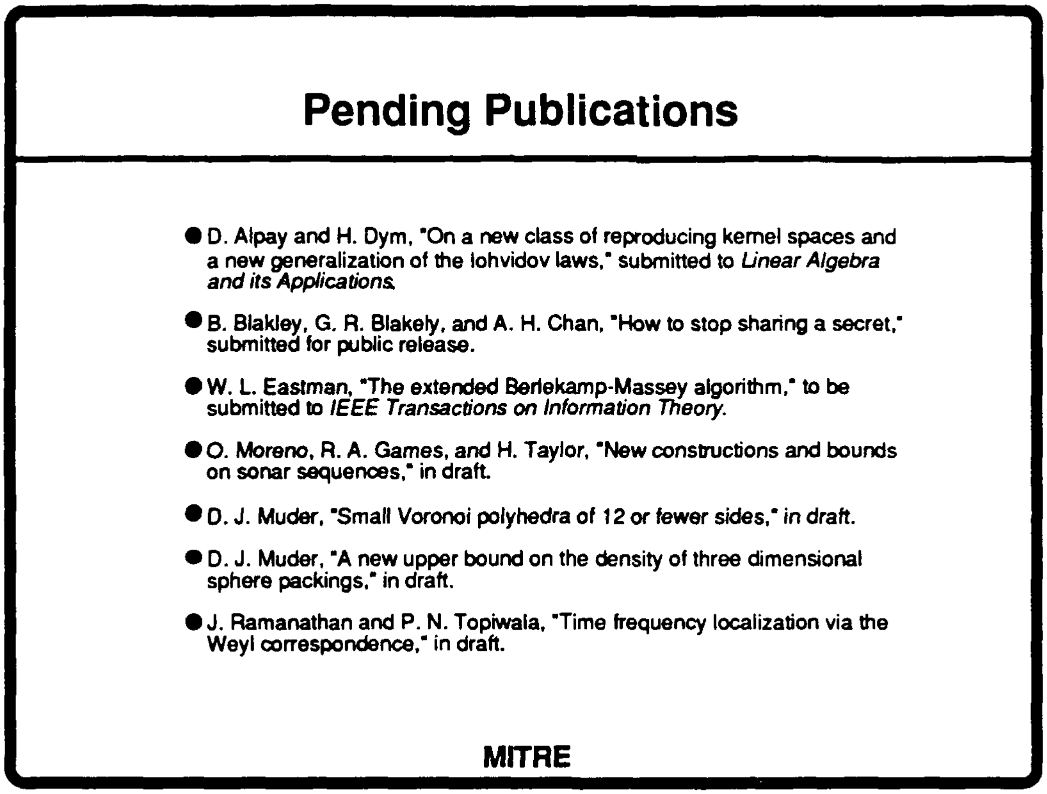
  Wavelets for image processing (G030)

  Network management and control (G110)

MITRE

Application Initiatives

In addition to continuing these efforts, we will continue to broaden the impact of our work within MITRE. We plan to work with the image processing group to explore the application of wavelets, a new time-scale transformation, to MITRE's imaging work. We will collaborate with the network management group in identifying opportunities for the application of our expertise in discrete mathematics to control problems associated with computer networks of growing complexity. Project personnel will continue to solve mathematical problems that arise in other MITRE projects.



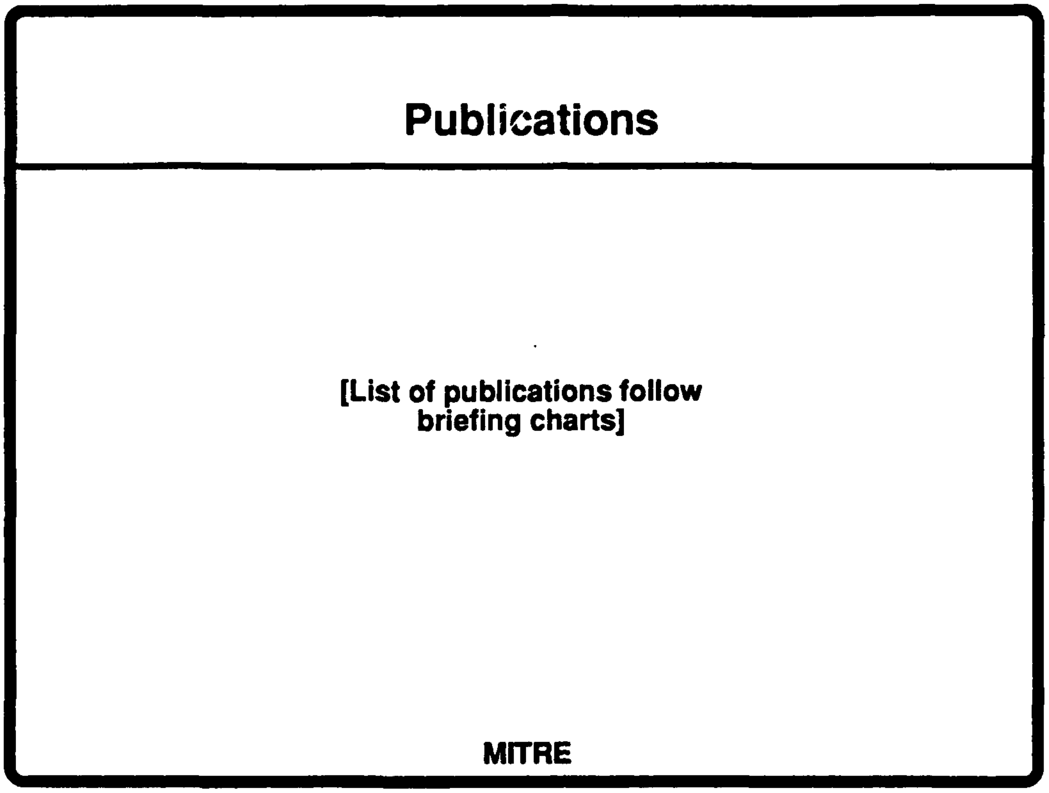
Pending Publications

- D. Alpay and H. Dym, "On a new class of reproducing kernel spaces and a new generalization of the Iohvidov laws," submitted to *Linear Algebra and its Applications.*
- B. Blakley, G. R. Blakely, and A. H. Chan, "How to stop sharing a secret," submitted for public release.
- W. L. Eastman, "The extended Berlekamp-Massey algorithm," to be submitted to *IEEE Transactions on Information Theory.*
- O. Moreno, R. A. Games, and H. Taylor, "New constructions and bounds on sonar sequences," in draft.
- D. J. Muder, "Small Voronoi polyhedra of 12 or fewer sides," *in draft.*
- D. J. Muder, "A new upper bound on the density of three dimensional sphere packings," in draft.
- J. Ramanathan and P. N. Topiwala, "Time frequency localization via the Weyl correspondence," in draft.

MITRE

Pending Publications

A list of external publications that are being generated in FY91.



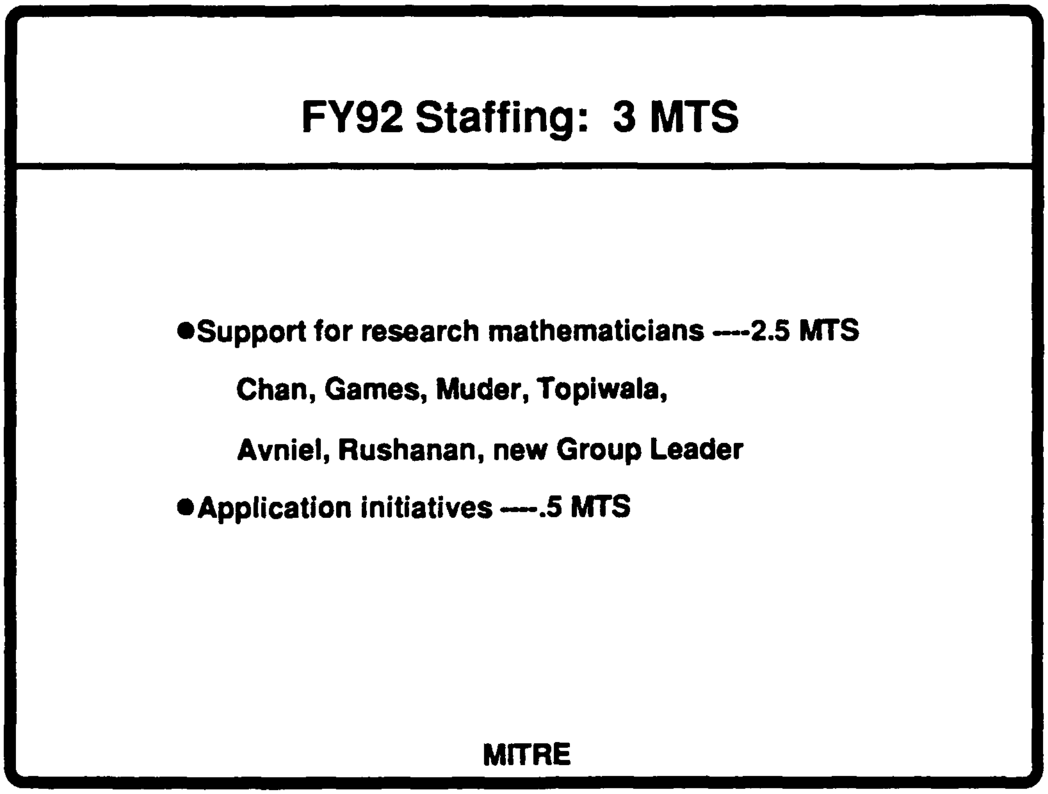
Publications

[List of publications follow
briefing charts]

MITRE

Publications

A list of external publications that have been generated by the project over the years.



FY92 Staffing: 3 MTS

- Support for research mathematicians ----2.5 MTS

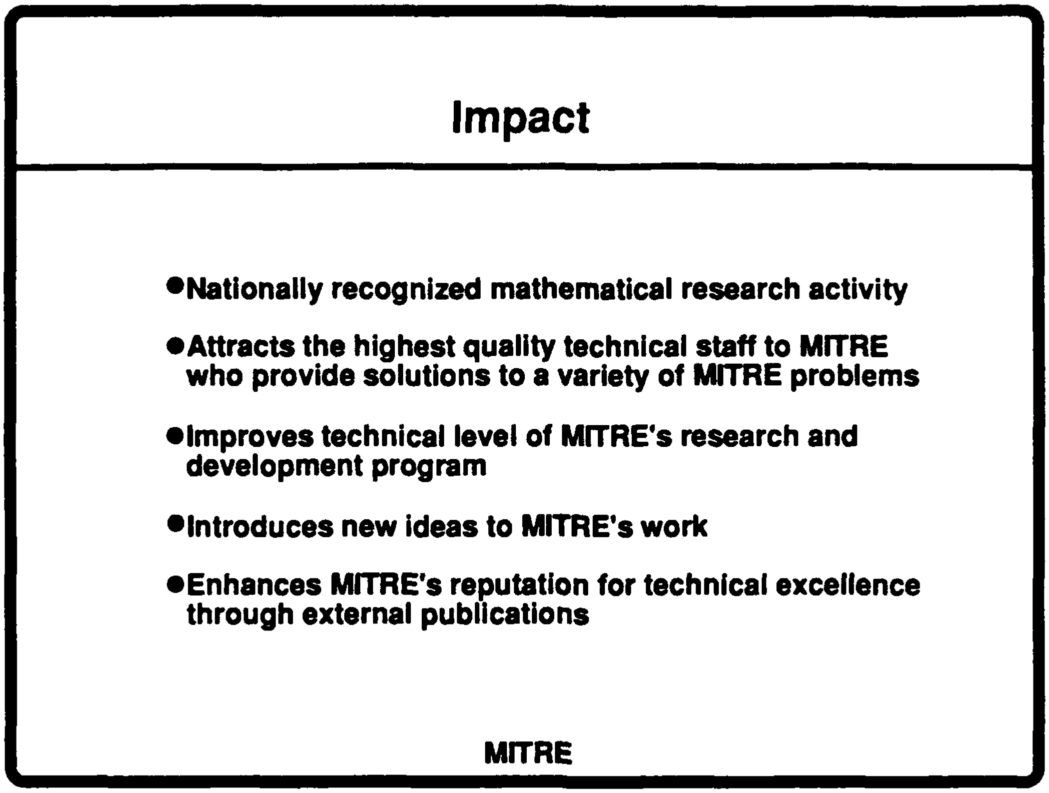
  Chan, Games, Muder, Topiwala,

  Avniel, Rushanan, new Group Leader
- Application initiatives ----.5 MTS

MITRE

FY92 Staffing: 3 MTS

The proposed staffing level along with potential staff; to be supported part time.



Impact

- Nationally recognized mathematical research activity
- Attracts the highest quality technical staff to MITRE who provide solutions to a variety of MITRE problems
- Improves technical level of MITRE's research and development program
- Introduces new ideas to MITRE's work
- Enhances MITRE's reputation for technical excellence through external publications

MITRE

Impact

We will continue our contributions toward the effective formulation and solution of mathematical problems that arise at MITRE. The results of this project will continue to be disseminated through internal seminars and reports, conference presentations, and publications in professional journals. A high level of research activity in applied mathematics will be maintained, bringing new ideas to bear on MITRE's work and enhancing MITRE's reputation for excellence.

External Publications of the MITRE Mathematical Research Project

Papers are listed by year of submission. Most of the papers listed below report work performed at MITRE and were published in refereed journals. The exceptions are papers published in conference proceedings, which are marked with an asterisk, and papers written at MITRE but reporting work done outside of MITRE, which are marked with a double asterisk. Papers that have not yet been published are marked as "submitted" or "to appear," depending on their status. Three of the papers won MITRE Best Paper awards: No. 8 in 1985, No. 20 in 1988, and No. 17 in 1990.

Prehistory

1. A. H. Chan and R. A. Games, "(n, k, t)-covering systems and error-trapping decoding," *IEEE Transactions on Information Theory* **IT-27** (1981), 643-646.

2. A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of de Bruijn sequences," *Journal of Combinatorial Theory (A)* **33** (1982), 233-246.

*3. A. H. Chan, R. A. Games, and E. L. Key, "On the complexities of periodic sequences," *Annals of Discrete Mathematics* **17** (1983), 159-170.

4. A. H. Chan and R. A. Games, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Transactions on Information Theory* **IT-29** (1983), 144-146.

FY82

*5. J. H. Rabinowitz, "De Bruijn sequences and hypergraphs over finite alphabets," *Congressus Numerantium* **36** (1982), 93-113.

FY83

6. T. J. Ferguson and J. H. Rabinowitz, "Self-synchronizing Huffman codes," *IEEE Transactions on Information Theory* **IT-30** (1984), 687-693.

7. V. K. Proulx and J. H. Rabinowitz, "An asymptotic approach to the channel assignment problem," *SIAM Journal on Algebraic and Discrete Methods* **6** (1985), 507-518.

FY84

8. J. H. Cozzens and L. A. Finkelstein, "Computing the discrete Fourier transform using residue number systems in a ring of algebraic integers," *IEEE Transactions on Information Theory* **IT-31** (1985), 580-588.

9. R. A. Games, "Complex approximations using algebraic integers," *IEEE Transactions on Information Theory* **IT-31** (1985), 565-579.

FY85

10. A. H. Chan, "Using decision trees to derive the complement of a binary function with multiple-valued inputs," *IEEE Transactions on Computers* **C-36** (1987), 212-

11. R. A. Games, "Optimal book embeddings of the baseline, Beneš, and barrel-shifter networks," *Algorithmica* **1** (1986), 233-250.

12. R. A. Games, "An algorithm for complex approximations in $\mathbf{Z}[e^{2\pi i/8}]$," *IEEE Transactions on Information Theory* **IT-32** (1986), 603-607.

13. D. J. Muder, "Concerning a conjecture of Colliot-Thélène and Sansuc," *Duke Mathematical Journal* **55 (1987), 51-63.

14. D. J. Muder, M. L. Weaver, and D. B. West, "Pagenumber of complete bipartite graphs I," *Journal of Graph Theory* **12** (1988), 469-489.

FY86

15. M. F. Bridgland, "Universal Traversal Sequences for Paths and Cycles," *Journal of Algorithms* **8** (1987), 395-404.

*16. A. H. Chan and R. A. Games, "On the linear span of binary sequences obtained from finite geometries," *Advances in Cryptology—CRYPTO '86, Lecture Notes in Computer Science* **263** Springer, Berlin-New York (1987), 405-417.

17. A. H. Chan and R. A. Games, "On the linear span of binary sequences obtained from q-ary M-sequences, q odd," *IEEE Transactions on Information Theory* **IT-36** (1990), 548-552.

18. J. H. Cozzens and L. A. Finkelstein, "Range and error analysis for an FFT computed over $\mathbf{Z}[\omega]$," *IEEE Transactions on Information Theory* **IT-33** (1987), 582-590.

19. R. A. Games, "An algebraic construction of sonar sequences using M-sequences," *SIAM Journal on Algebraic and Discrete Methods* **8** (1987), 753-761.

20. D. J. Muder, "Putting the best face on a Voronoi polyhedron," *Proceedings of the London Mathematical Society* (3) **56** (1988), 329-348.

FY87

*21. M. F. Bridgland and R. J. Watro, "Fault-tolerant distributed decision making in totally asynchronous distributed systems (preliminary version)," in *Proceedings of the Sixth Annual ACM Symposium on the Principles of Distributed Computing*, 1987, 52-63.

22. D. J. Muder, "Minimal trellises for block codes," *IEEE Transactions on Information Theory* **IT-34** (1988), 1049-1053.

FY88

23. D. J. Muder, "How big is an n-sided Voronoi polygon?" *Proceedings of the London Mathematical Society* (3) **61** (1990), 91-108.

FY89

24. A. H. Chan and R. A. Games, "On the quadratic spans of DeBruijn sequences," *IEEE Transactions on Information Theory* **IT-36** (1990), 822-829.

*25. A. H. Chan and R. A. Games, "On the quadratic spans of periodic sequences," *Advances in Cryptology—CRYPTO '89, Lecture Notes in Computer Science* **435** Springer, Berlin-New York (1990), 82-89.

26. J. Ramanathan, "Minimal hypersurfaces in S^4 with vanishing Gauss-Kronecker curvature," *Mathematische Zeitschrift* (1990), **205, 645-658.

**27. J. J. Rushanan, "Duadic codes and difference sets," *The Journal of Combinatorial Theory* (to appear).

**28. J. J. Rushanan, "Eigenvalues and the Smith normal form," *Linear Algebra and Its Applications* (submitted).

FY90

29. J. Ramanathan and O. Zeitouni, "On the wavelet transform of fractional Brownian motion," *IEEE Transactions on Information Theory* **IT-39** (1991).