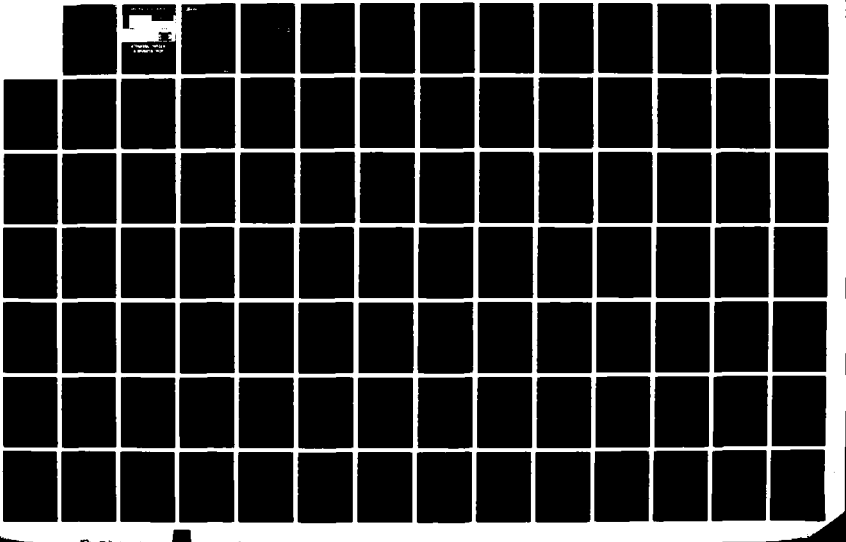
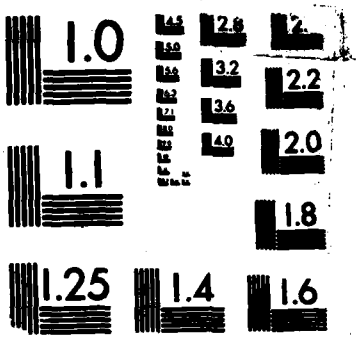
AD-A193 252 IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY (ISIT): ABSTRACTS OF P.. (U) MICHIGAN UNIV ANN ARBOR ROBINSON OCT 86 AFOSR-TR-88-0287 AFOSR-87-0046 1/3

UNCLASSIFIED F/G 12/9 NL





MICROCOPY RESOLUTION TEST CHART
URFAU OF STANDARDS-1963-A

INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY

October 6-9, 1986

Ann Arbor,
Michigan, USA

SPONSORED BY: IEEE INFORMATION THEORY GROUP

IEEE Catalog Number 86 CH 2374-7

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY: UNCLASSIFIED	3. DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release, distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S): AFOSR-TR- 88-0287
6a. NAME OF PERFORMING ORGANIZATION: University of Michgan; 6b. OFFICE SYMBOL (If applicable)	7a. NAME OF MONITORING ORGANIZATION: AFOSR
6c. ADDRESS (City, State and ZIP Code): The Institute of Electrical and Engineering Electronic, Ann Arbor, Michgan	7b. ADDRESS (City, State and ZIP Code): BLDG #410 Bolling AFB, DC 20332-6448
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: AFOSR; 8b. OFFICE SYMBOL (If applicable): NM	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER: AFOSR- 87-0046
8c. ADDRESS (City, State and ZIP Code): BLDG #410 Bolling AFB, DC 20332-6448	10. SOURCE OF FUNDING NOS.

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT NO.
61102F	2304	A6	

11. TITLE (Include Security Classification): 1986 IEEE International Symposium on Information Theory

12. PERSONAL AUTHOR(S): Robinson

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Yr., Mo., Day)	15. PAGE COUNT
Final	FROM Oct 86 TO Oct 9, 86	Oct 86	

16. SUPPLEMENTARY NOTATION: decentralized detection,

17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB. GR.	

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

The 1986 IEEE

The 1986 IEEE International Symposium on Information Theory was held October 6-9, 1986 at the University of Michgan in Ann Arbor, Michgan. There were 274 papers presented in a variety areas related to information theory, including multiple-access channels, estimation and ~~detection~~, coding theory, random processes, data compression, quantization, and speech and image processing.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION
UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT ☐ DTIC USERS ☐	UNCLASSIFFIED

22a. NAME OF RESPONSIBLE INDIVIDUAL	22b. TELEPHONE NUMBER (Include Area Code)	22c. OFFICE SYMBOL
Brian W. Woodruff, Maj	202-767-5027	

DD FORM 1473, 83 APR — EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

1986 IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY (ISIT)

UNIVERSITY of MICHIGAN
ANN ARBOR, MICHIGAN

OCTOBER 6-9, 1986

Sponsored by:

The Institute of Electrical
and Electronic Engineers,
Information Theory Group

Co-Chairmen

F. J. Beutler D. L. Neuhoff

Vice-Chairman

A. D. Wyner

International Advisory Committee

L. Campbell	(Canada)
A. B. Carleial	(Brazil)
S. Csibi	(Hungary)
G. Dueck	(West Germany)
P. G. Farrell	(United Kingdom)
H. Guoding	(China)
R. Johannesson	(Sweden)
M. Kasahara	(Japan)
F. Kuhlmann	(Mexico)
A. Lempel	(Israel)
T. Maseng	(Norway)
O. Moreno	(Puerto Rico)
J. M. F. Moura	(Portugal)
E. Panayirci	(Turkey)
B. Picinbono	(France)
P. Piret	(Belgium)
W. L. Root	(USA)
A. Sgarro	(Italy)
B. S. Tsybakov	(USSR)
G. Ungerboeck	(Switzerland)

Library of Congress #72-179437

Program Chairman

S. C. Schwartz

Program Committee

R. Blahut
I. Blake
A. Ephremides
D. Goodman
C. Heegard
N. Mehravari
J. Modestino
H.V. Poor
M.B. Pursley
N. Sloane
P. Swaszek
J. Thomas
S. Verdú
J. Wolf
A. Wyner

Local Arrangements Chairman: W. Stark

Publications Chairmen: D. Teneketzis, G. H. Wakefield

Publicity Chairman: A. O. Hero

Symposium Treasurer: S. R. Robinson

PROGRAM SCHEDULE

Day	Time Period	Activity*
Sunday	5-8 pm	Registration
	7-9:30 pm	Reception
Monday	8-11 am	Registration
	8:30-9:30 am	Plenary Lecture†
	9:30-10:00 am	Coffee Break
	10:00-11:40 am	"A"-Sessions
	12:00-1:15 pm	Luncheon at League
	1:30-3:10 pm	"B"-Sessions
	3:10-3:30 pm	Coffee Break
	3:30-5:10 pm	"C"-Sessions
	7:30-9:30 pm	Cash Bar
	8:00-9:00 pm	Concert
Tuesday	8:30-9:30 am	Plenary Lecture†
	9:30-9:45 am	Coffee Break†
	9:45-10:45 am	Shannon Lecture†
	11:00-12:20 am	"A"-Sessions
	12:30-1:45 pm	Luncheon at League
	2:00-3:20 pm	"B"-Sessions
	3:20-3:40 pm	Coffee Break
	3:40-5:20 pm	"C"-Sessions
	8:00-10:30 pm	Cash Bar with Music
	8:30-10:00 pm	Recent Results Session
Wednesday	8:30-9:30 am	Plenary Lecture†
	9:30-9:50 am	Coffee Break
	9:50-11:30 am	"A"-Sessions
	1:00-5:00 pm	Greenfield Village (or Henry Ford Museum)
	7:00-8:00 pm	Cash Bar for Banquet
	8:00-9:30 pm	Banquet
Thursday	8:30-9:30 am	Plenary Lecture†
	9:30-10:00 am	Coffee Break
	10:00-11:40 am	"A"-Sessions

*Unless otherwise noted, activity will be at the Michigan League.

†At Rackham Auditorium.

1:40-3:00 pm	"B"-Sessions
3:00-3:30 pm	Coffee Break
3:30-4:50 pm	"C"-Sessions

PROGRAM

TABLE OF CONTENTS

PROGRAM

MA3 - QUANTIZATION I

MA4 - PERFORMANCE BOUNDS FOR TRELLIS AND CONVOLUTIONAL CODES

MA5 - ESTIMATION THEORY - APPLICATIONS

PROGRAM

PROGRAM

MB2 - MAGNETIC RECORDING I

MB3 - RANDOM PROCESSES I

MB4 - OPTICAL COMMUNICATIONS I

PROGRAM

MC2 - MAGNETIC RECORDING II

MC3 - SPEECH AND IMAGE PROCESSING

MC4 - COMMUNICATION SYSTEMS

PROGRAM

MC5 - BLOCK DECODING

MC6 - SHANNON THEORY I

MC7 - ESTIMATION AND IDENTIFICATION

PROGRAM

TUESDAY, OCTOBER 7, 1986

8:30 am - 9:30 am PLENARY LECTURE

9:30 am - 9:45 am COFFEE BREAK

9:45 am - 10:45 am SHANNON LECTURE

11:00 am - 12:20 pm "A" SESSIONS

TA1 - PATTERN RECOGNITION I

TA2 - CONSTRUCTION OF TRELLIS CODES

TA3 - QUEUEING THEORY AND QUEUEING NETWORKS

PROGRAM

PROGRAM

12:30 pm - 1:45 pm LUNCHEON AT LEAGUE

2:00 pm - 3:20 pm "B" SESSIONS

TB1 - PATTERN RECOGNITION II

TB2 - ALGEBRAIC CODING

TB3 - NETWORKS: PROTOCOLS AND FLOW CONTROL

PROGRAM

TB4 - CODES IN EUCLIDEAN SPACE

TB5 - INVESTMENT AND GAMBLING THEORY

TB6 - SHANNON THEORY III

3:20 pm - 3:40 pm COFFEE BREAK

3:40 pm - 5:20 pm "C" SESSIONS

TC1 - CONSTRUCTION OF CONVOLUTION AND TRELLIS CODES

PROGRAM

TC2 - OPTICAL COMMUNICATIONS II

TC3 - RANDOM PROCESSES II

TC4 - CONTINUOUS PHASE MODULATION

PROGRAM

PROGRAM

WA5 - DETECTION THEORY II

WA6 - SEQUENCES I

THURSDAY, OCTOBER 9, 1986

8:30 am - 9:30 am PLENARY LECTURE

PROGRAM

9:30 am - 10:00 am COFFEE BREAK

10:00 am - 11:40 am "A" SESSIONS

THA1 - ALGORITHMS AND COMPLEXITY

THA2 - SOURCE CODING III

THA3 - RANDOM ACCESS COMMUNICATIONS II

PROGRAM

PROGRAM

THA7 - SEQUENCES II

1:40 pm - 3:00 pm "B" SESSIONS

THB1 - MULTIDIMENSIONAL CODES

THB2 - TRELLIS DECODERS

PROGRAM

THB3 - MULTIPLE ACCESS COMMUNICATIONS

THB4 - SYNCHRONIZATION

THB5 - CODING II

PROGRAM

THB6 - SHANNON THEORY V

3:00 pm - 3:30 pm COFFEE BREAK

3:30 pm - 4:50 pm "C" SESSIONS

THC1 - APPLICATIONS OF INFORMATION THEORY

THC2 - ALGEBRAIC CODING THEORY II

PROGRAM

THC3 - CODING FOR SPECIAL CHANNELS

THC4 - DATA COMPRESSION

THC5 - SEQUENTIAL DECODING

THC6 - SHANNON THEORY VI

PROGRAM

MONDAY

	1	2	3	4	5	6	7
A	Multiple-Access Channels: Capacity	Computer Applications of Coding	Quantisation I	Performance Bounds for Trellis and Convolutional Codes	Estimation Theory - Applications	VLSI and Systolic Arrays	Decentralised Detection
B	Source Coding I	Magnetic Recording I	Random Processes I	Optical Communications I	Random Access Communications I	Algebraic Coding Theory I	--
C	Coding I	Magnetic Recording II	Speech and Image Processing	Communication Systems	Block Decoding	Shannon Theory I	Estimation and Identification

TUESDAY

	1	2	3	4	5	6
A	Pattern Recognition I	Construction of Trellis Codes	Queueing Theory and Queueing Networks	Detection Theory I	Block Code Performance	Shannon Theory II
B	Pattern Recognition II	Algebraic Coding	Networks: Protocols and Flow Control	Codes in Euclidean Space	Investment and Gambling Theory	Shannon Theory III
C	Construction of Convolution and Trellis Codes	Optical Communications II	Random Processes II	Continuous Phase Modulation	Filtering	Shannon Theory IV

WEDNESDAY

	1	2	3	4	5	6
A	Construction of Modulation Codes	Cryptography	Coding Techniques	Source Coding II	Detection Theory II	Sequences I

THURSDAY

	1	2	3	4	5	6	7
A	Algorithms and Complexity	Source Coding III	Random Access Communications II	Bandwidth and Synchronisation of Codes	Quantisation II	Detection and Estimation	Sequences II
B	Multidimensional Codes	Trellis Decoders	Multiple Access Communications	Synchronisation	Coding II	Shannon Theory V	--
C	Applications of Information Theory	Algebraic Coding Theory II	Coding for Special Channels	Data Compression	Sequential Decoding	Shannon Theory VI	--

PLENARY LECTURE*

SPEECH RECOGNITION BY STATISTICAL METHODS,

FREDERIC JELINEK, Continuous Speech Recognition Group, Dept. of Computer Sciences, IBM Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598, USA.

The Speech Recognition Group at the IBM Thomas J. Watson Research Center has recently completed the implementation of a real-time, IBM-PC based, large vocabulary speech recognition system that can be used for dictating office correspondence. To make real time performance possible, the vocabulary is restricted to 5,000 words that must be spoken with short pauses between them.

The system is based on an information theoretical (rather than expert system) formulation of the recognition problem. The algorithms used are statistical and all the parameters of the system are estimated directly from data.

In this talk, the basic theory behind the recognizer will be presented with special emphasis on the language model component which provides the probability of the next word, given the past hypothesis. The talk will be accompanied by a live demonstration of the recognizer.

*Plenary Lectures will be given in the *Horace H. Rackham Building Lecture Hall*, East Washington Street between State and Fletcher streets.

SESSION MA1

MULTIPLE-ACCESS CHANNELS: CAPACITY

SYMBOL-ASYNCHRONOUS GAUSSIAN MULTIPLE ACCESS CHANNELS,

SERGIO VERDÚ, Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA.

Frame-asynchronism has no effect on the capacity region of the Gaussian multiple-access channel (MAC). This is the only type of asynchronism under which the MAC has been analyzed. We show that symbol-asynchronism, which represents the case where transmitters are completely asynchronous and their symbol-epochs do not coincide, affects channel capacity in a fundamental way. Symbol-asynchronism arises when users transmit each codeword symbol by modulating an assigned waveform and they do not cooperate in order that the beginning of each symbol transmission coincides. To encompass multi-user communication systems where each user is not assigned the same waveform a more general model than the scalar Gaussian MAC has to be adopted by modeling the sufficient statistics observed by the decoder as a K-vector discrete-time process. The symbol-asynchronous channel has finite memory because each transmitted symbol affects two consecutive observed vectors; also, it is a decoder-informed compound channel since the encoders do not know the timing of the other users, and hence they ignore the waveform crosscorrelations which determine the degree of interference among them. The derivation of the symbol-asynchronous capacity region shows several interesting features. Unlike the conventional Gaussian MAC there is no input distribution maximizing all mutual information constraints on the rate-sums, and in the two-user case the capacity region is no longer a pentagon. For high SNR there are simple closed-form expressions which quantify the fundamental limitation on the speed of reliable transmission imposed by the existence of other asynchronous users. [This work was partially supported by the National Science Foundation under Grant ECS-8504752.]

SEQUENTIAL DECODING FOR MULTIPLE ACCESS CHANNELS,

ERDAL ARIKAN, Coordinated Science Laboratory and the Department of Electrical Engineering, University of Illinois at Urbana-Champaign, 1101 West Springfield Avenue, Urbana, IL 61801, USA.

Application of sequential decoding to multiple access channels is considered. The main contribution is the introduction of a new metric (a measure of statistical correlation that the algorithm uses to find the correct message), and the finding of an inner bound to the rate region where this metric can be used. The results indicate that the achievable rate region of sequential decoding is larger than the achievable rate regions of such common techniques as time-division multiplexing, frequency division multiplexing, and Aloha-like schemes. [The research was conducted at M.I.T. Laboratory for Information and Decision Systems with support provided by Defense Advanced Research Projects Agency under Contract N000 14-84-K-0357.]

SOME RESULTS ON ERROR PROBABILITY AND FREE DISTANCE BOUNDS FOR TWO-USER TREE AND TRELLIS CODES ON MULTIPLE ACCESS CHANNELS,

ZHONGXING YE, Center for Applied Mathematics, Cornell University, Ithaca, NY 14853, USA, and Mathematics Department, Nankai University, Tianjin, PRC and TOBY BERGER, School of Electrical Engineering and Center for Applied Mathematics, Cornell University, Ithaca, NY 14853, USA.

1. A class of terminated trellis codes is considered for use on an arbitrary two-user discrete memoryless multiple channel (MAC). At the decoder a two-user trellis is employed to achieve ML decoding. We distinguish nine possible decoding error event types. An upper bound on the total ML decoding error probability is obtained. It approaches zero exponentially with increasing code constraint length for all rate pairs within the two-user capacity region. A lower bound on free distance for this class of trellis codes is derived using the same technique.

2. A superposition compound tree coding method is considered for a discrete memoryless MAC with correlated sources. Two decoding methods (called one-step and two-step decoding) are suggested. The upper bounds of ML decoding error probabilities are obtained for these two cases. They approach zero exponentially as the tail length of the tree code increases. The merits and demerits of the two methods are compared.

TWO RESULTS ON MULTIPLE-ACCESS CHANNELS,

KRISTIEN DE BRUYN, EDWARD C. VAN DER MEULEN, and PETER VANROOSE, Department of Mathematics, Katholieke Universiteit Leuven, Celestijnenlaan 200 B, B-3030 Leuven, Belgium.

First it is shown that the capacity region of the discrete memoryless multiple-access channel with correlated sources in the sense of Slepian and Wolf (1973) with feedback equals the achievable rate region found by King (1978), when the multiple-access channel belongs to the class recently defined by Hekstra and Willems (1984) who proved that for channels in this class the Cover-Leung (1981) region is the capacity region of the discrete memoryless multiple-access channel with two independent input users and feedback.

Secondly, all deterministic multiple-access channels with two input users and binary inputs are considered and classified. One particular deterministic multiple-access channel, not recently studied, is thereby analyzed. This channel differs from the binary adder channel studied by Kasami and Lin (1976, 1978, 1983) and the noiseless OR-channel considered by Gyorfi and Kerekes (1981). For this particular deterministic multiple-access channel under consideration a class of uniquely decodable codepairs is constructed yielding rate pairs well above the time-sharing line.

GAUSSIAN MULTIPLE ACCESS CHANNEL CAPACITY CAN AT MOST BE DOUBLED BY FEEDBACK,

JOY A. THOMAS, Department of Electrical Engineering, Stanford University, Stanford, CA 94305, USA.

Gaarder and Wolf first demonstrated that feedback enables the senders in a multiple access channel to cooperate and hence increases capacity. In this paper, we generalize the converse for the multiple access channel with feedback and use it to obtain strong bounds on the capacity (sum of the rates of all the senders) of an m-user Gaussian multiple access channel in terms of the covariance matrix of its inputs. We use these bounds to show that the capacity of the channel with feedback is less than twice the capacity without feedback.

We also use the converse for the general multiple access channel to show that for any m-user multiple access channel, feedback cannot increase the capacity by more than a factor of m. [This work was partially supported by the National Science Foundation under Grant ECS82-11568 and the Defense Advanced Research Projects Agency under Contract N00039-84-C-0211.]

NOTES

SESSION MA2

COMPUTER APPLICATIONS OF CODING

EXHAUSTIVE TEST PATTERN GENERATION USING CYCLIC CODES,[+]

C.L. CHEN, International Business Machines Corporation, Department D18, Building 707, P.O. Box 390, Poughkeepsie, NY 12602, USA.

The generation of exhaustive test patterns for very large scale integration (VLSI) circuits using linear feedback shift registers is described in terms of cyclic codes. Punctured cyclic codes are used to generate exhaustive test patterns of any length. A technique for the generation of punctured cyclic codes is presented. A new technique is also presented for the generation of exhaustive test patterns that yields test sets of smaller size.

THE USE OF TWO-DIMENSIONAL CODES IN THE RECONSTRUCTION OF A CORRECT FILE COPY FROM MULTIPLE ERRONEOUS COPIES,

JOHN J. METZNER, Oakland University, School of Engineering and Computer Science, Rochester, MI 48063, USA.

The problem of obtaining a correct copy of a file of data from two or more erroneous copies is common to the following three applications: (1) *retransmission* of a file; (2) *broadcast* of a file of data to two or more receivers; (3) maintenance of *backup* file copies. In this paper, a technique is proposed whereby each file is error detection coded in a two-dimensional array. Parity bits are provided for each row and column (plus an additional parity sequence for assured overall error detection). For two file copies A and B, suppose each reports to the other the rows which do not check. Rows which check at B but not at A are sent from B to A, and vice versa. Every exchange row removes at least one error. If errors remain, the same procedure is followed with the columns. Sometimes additional errors are eliminated by repeating the process. Also, the two-dimensional array structure itself permits further error correction.

An analysis is made of the error reduction as a function of bit error probability, number of copies, and file size. For the case of two copies of a 40k bit file, It will usually be possible to correct random patterns of about 80 random errors in each file with rather simple procedures. In some of the applications, a secondary goal may be to obtain the corrections with a minimum amount of communication. Analysis of the amount of communication required indicates that the number of errors times the number of bits in a row is a rather tight bound on the amount of communication.

[+]Denotes Long Paper

THE EFFECT OF SOFT ERROR SCRUBBING ON SINGLE-ERROR PROTECTED RAM SYSTEMS,

MARIO BLAUM, IBM Almaden Research Center, San Jose, CA 95120, USA, and
RODNEY M. GOODMAN and ROBERT J. McELIECE, Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125, USA.

This paper is concerned with assessing the reliability of coded computer memories. Each row of chips in the memory is protected by a single-error-correcting double-error-detecting code, and we wish to estimate the improvement in system mean time to failure (MTTF) due to the use of coding. In particular we extend our previous work which covered the case of hard errors only, to include the technique of soft error scrubbing. In the paper we derive bounds on the improvement to be gained by soft error scrubbing and show that depending on the relative proportions of the interval chip failure modes, scrubbing may or may not be useful. Also we derive a reliability expression that incorporates the scrubbing interval T as a parameter, and tie together the analytical results by comparing them to extensive simulations.

AN ERROR-CONTROL CODING SYSTEM FOR STORAGE OF 16-BIT WORDS IN MEMORY ARRAYS COMPOSED OF THREE 9-BIT WIDE UNITS,

WIL J. VAN GILS, Philips Research Laboratories, P.O. Box 80.000, 5600 JA Eindhoven, The Netherlands.

Error-correcting codes are widely used to improve the reliability of computer memories. The shift of VLSI technology towards higher levels of integration has resulted in multiple-bit-per-card and multiple-bit-per-chip memory structures. This paper describes codes for storing 16-bit words in a memory array consisting of three 9-bit wide memory units, a unit being a single card or a single chip. These codes are able to correct single bit errors, detect up to four bit errors, and detect the failure of a complete memory unit. The codes have an elegant structure which makes fast decoding possible by simple means.

SESSION MA3

QUANTIZATION I

WEIGHTED PYRAMID AND ELLIPTICAL VECTOR QUANTIZERS,

THOMAS R. FISCHER, Department of Electrical Engineering, Texas A&M University, College Station, TX 77843, USA.

For the Laplacian and correlated Gaussian sources, the regions of high probability important for source coding are the weighted pyramid and ellipse, respectively. By selecting code words as the intersection of the points in a suitable lattice with the region of high probability, very effective vector quantizers can be constructed. Such vector quantizers offer the advantages of scalar quantization combined with entropy coding, but with fixed-length code words, the simplified quantization procedure associated with lattices, and the reduction in mean-squared error that certain lattices provide, compared to the mean-squared error of the uniform lattice.

Constructive algorithms are presented for the design of vector quantizers based on the geometries on the weighted pyramid and the ellipse. Performance expressions are derived for these vector quantizers and compared to the optimum scalar quantizer and the distortion-rate bound.

PERFORMANCE ANALYSIS OF A FAST VECTOR QUANTIZATION SCHEME,

NADER MOAYERI, DAVID L. NEUHOFF, and WAYNE STARK, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109, USA.

In earlier work we proposed a fast quantization rule for the codebook $\mathbf{C}$ of a given vector quantizer (VQ), and obtained experimental results in applying this technique to a number of codebooks designed for a variety of sources. First, a source vector is quantized by a fine VQ for which there is a fast quantization algorithm. Second, a table look-up finds the closest (in distortion) quantization vector of the original codebook $\mathbf{C}$ to that found by the fine quantization.

In this paper we study the increase in the average distortion when the suboptimum fast rule is used instead of the minimum distortion rule and the fine quantizer is a lattice code. Purely geometric upper bounds are given to the increase in average distortion. Moreover, for a reasonably fine lattice code (not necessarily rectangular), we derive an approximate formula for the performance loss, which clearly separates the effects of the source distribution and the geometry of $\mathbf{C}$ from the effects of size and shape of the lattice cells.

NEW ALGORITHMS FOR OPTIMUM QUANTIZATION AND $\bar{\rho}$-DISTANCE,

WILLIAM PEARLMAN, Department of Electrical Engineering, Technion - Israel Institute of Technology, Technion City, Haifa 32000, Israel.

Alphabet-constrained rate distortion functions with computational algorithms provide a convenient vehicle for computation of optimum quantizer characteristics and $\bar{\rho}$-distance. The minimum distortion point of a rate-distortion function constrained by reproduction alphabet size yields the output entropy of the corresponding Lloyd-Max quantizer. The computational algorithm yields not only the distortion and rate, but a set of transition and output probabilities determining the decision and reproduction values of the quantizer. Furthermore, a simple modification of the distortion measure in each step of the algorithm allows convergence to a point on the optimum entropy-coded quantizer rate-versus-distortion curve for the given number of reproduction values. Calculations confirm convergence to known minimum distortion and optimum (entropy-coded) quantizer characteristics. Another rate-distortion function can be defined where the full reproduction ensemble (letters and probabilities) is fixed. The minimum distortion point of this function is the $\bar{\rho}$-distance between the source and reproduction ensembles. Calculations of $\bar{\rho}$-distances using discrete and continuous ensembles are carried out through a convergent fixed point algorithm for this fully constrained-alphabet rate-distortion function. No algorithm for computing $\bar{\rho}$-distance has been reported previously.

OPTIMAL QUANTIZER DESIGN FOR NOISY CHANNELS,

N. FARVARDIN and V. VAISHAMPAYAN, Electrical Engineering Department and Systems Research Center, University of Maryland, College Park, MD 20742, USA.

In this paper, we present an analysis of the zero-memory quantization of memoryless sources when the quantizer output is to be encoded and transmitted across a noisy channel. Necessary conditions for the joint optimization of the quantizer and the encoder/decoder pair are presented and an iterative algorithm for obtaining a locally optimal system is developed. The performance of this locally optimal system, obtained for the class of generalized Gaussian distributions and the Binary Symmetric Channel is compared against the optimum performance theoretically attainable (using rate-distortion theoretic arguments), as well as against the performance of the Lloyd-Max quantizers encoded using Natural Binary Codes. It is shown that this optimal design could result in substantial performance improvements. The performance improvements are more noticeable at high bit rates and for more broad-tailed densities. [This work was supported by grants from Martin Marietta Laboratories and NSF CDR-85-00108.]

OVERSAMPLED SIGMA DELTA MODULATION FOR SCALAR QUANTIZATION,

ROBERT M. GRAY, Information Systems Laboratory, Department of Electrical Engineering, Stanford University, Stanford, CA 94305-2099, USA.

Oversampled sigma delta modulation has been proposed as a practical implementation for high rate PCM because of its simplicity and its robustness against circuit imperfections. All of the mathematical analyses for such systems, however, have been based either on simulations or on the assumption that the quantization error is is a uniformly distributed memoryless sequence that is independent of the input data. In particular, the stability of the system to a constant input and the accuracy of the system and its relation to uniform scalar quantization (PCM) is based entirely on simulation and the additive independent memoryless noise assumption. This assumption is not mathematically reasonable because the quantization takes place within a feedback loop and because it ha· a low bit rate, typically only one bit.

We present new results regarding the stability and performance of sing'e integrator sigma-delta modulators and their relation to uniform quantization assuming one bit quantizers and a large oversampling ratio. No assumptions are made regarding independence of the quantization noise and input or the memory in the noise. The techniques involve a simple but novel application of ergodic theory along with standard asymptotic quantization approximations. [This work was supported by NSF.]

NOTES

SESSION MA4

PERFORMANCE BOUNDS FOR TRELLIS AND CONVOLUTIONAL CODES

FREE DISTANCE RESULTS FOR FILTERED CONTINUOUS PHASE MODULATIONS WITH PRACTICAL FILTERS,

N. SESHADRI and J.B. ANDERSON, Electrical, Computer, and Systems Engineering Department, Rensselaer Polytechnic Institute, Troy, NY 12181, USA.

The effect of channel filtering on continuous phase modulation (CPM) is considered. Unlike most earlier work on channel filtering, we assume that the channel impulse response can be infinitely long. Using an algorithm developed for calculating the normalized minimum distance of modulations that are filtered by a rational transfer function, we obtain the distances for a variety of CPM schemes. Two- and four-pole Butterworth filtering is featured. Our results indicate that CPM with low modulation indices is not really bandwidth efficient. For larger indices, channel filtering does not necessarily degrade distance, and in fact can actually improve it. The effects of Butterworth filtering are similar to those we have reported earlier for ideal "brick wall" filtering. Results are presented for bandwidths down to $BT = 0.1$, where B is the single sideband RF bandwidth and T is the symbol duration.

ON THE PROBABILITY OF ERROR DUE TO METRIC TIES DURING VITERBI DECODING,

V. S̄ENK, DEJAN E. LAZIĆ, and T. BECE, Faculty of Technical Sciences, Institute for Measurement and Control, 21000 Novi Sad, V.Vlahovića 3, Yugoslavia.

The Viterbi algorithm (VA) resolves the metric ties between two or more mergers arbitrarily. The probability of error due to incorrect selection of a path after the metric tie has occurred is analyzed. We show that for a binary symmetric channel (BSC) the probability reaches about 10 percent of the entire error probability. We have conducted an extensive computer simulation of the performance of the VA for BSC's with and without memory, with different types of bursts and interleaving techniques, and observed the dependence of the error probability due to ties. The results of several deterministic tie-resolving techniques are compared with theoretical expectations.

BIT ERROR PROBABILITY CALCULATIONS FOR SHORT-CONSTRAINT LENGTH CONVOLUTIONAL CODES ON VERY NOISY CHANNELS,

L. HU, MARK A. HERRO, and DANIEL J. COSTELLO, Dept. of Electrical and Computer Engineering, University of Notre Dame, Notre Dame, IN 46556, USA.

Sub-optimum decoders are used to bound the bit error probability of maximum likelihood decoders on very noisy channels. Previous attempts to model the output of a maximum likelihood decoder as a stochastic process have used the technique of augmenting the number of states to reflect the dependence of the output sequence on all of the past inputs. Although this allows modeling the output of the decoder as a Markov process, it is usually impractical to implement since the number of required "states" grows rapidly with the constraint length of the code (e.g., 6 states for a (2,1,1) code and 104 states for a (2,2,2) code). We present a reduced state method that yields a Markov model of a simpler, sub-optimum decoder. This provides a lower bound on the bit error probability and the average error event length of the maximum likelihood decoder, since the performance of this decoder is necessarily sub-optimum. The interesting result is that this model provides a tighter bound on maximum likelihood decoding than the more direct attempts. The bound is tighter at low signal-to-noise ratios, but becomes weaker at high signal levels, because of the sub-optimum performance of the model decoder. [The work supported by NSF Grant ECS84-14608.]

PERFORMANCE ANALYSIS OF PERIODICALLY TIME VARYING PARTIAL RESPONSE SIGNALING WITH MAXIMUM LIKELIHOOD AND INTEGRATE & DUMP RECEIVERS,

REGINALDO PALAZZO, Jr., Electrical Engineering Dept., State University of Campinas, C.P. 6122, Campinas, S.P., Brazil.

An uncoded PAM communication system with periodically time varying controlled intersymbol interference is analyzed by use of the dynamic transfer function technique (DTFT) first developed to analyze convolutional codes. Under the assumption that all channel impulse responses have equal "energy," comparison between time invariant and periodically time varying controlled ISI is presented. It is shown that, for the controlled intersymbol interference with pulse duration $2T$, concentrating most of the pulse energy to any one of the equally spaced time interval, the periodic combination requires less signal-to-noise ratio to achieve the same performance as that of the time invariant with ISI under an optimum and suboptimum receiver. It is also shown that depending on the periodic combination of time invariant partial response signals, a small degradation is incurred by using periodically time varying partial response signals instead of those without ISI.

ON THE PERFORMANCE EVALUATION OF TRELLIS CODES,

EPHRAIM ZEHAVI, Qualcomm, San Diego, CA 92093, USA, and JACK K. WOLF, Center for Magnetic Recording Research, UCSD, and Qualcomm, San Diego, CA 92093, USA.

Generating function techniques for analyzing the error event and the bit error probabilities for trellis codes are considered. The conventional state diagram approach for linear codes where the number of states is equal to the number of trellis states cannot be applied directly to arbitrary trellis codes and instead, a state diagram where the number of states is equal to the square of the number of trellis states must be used. It is shown here that for an interesting class of trellis codes, a modified generating function can be defined, for which the number of states *is equal to* the number of trellis states.

The class of codes considered includes trellis codes of rate $R = (n-1)/n$, based upon set partitioning whenever the first partition breaks the signal constellation into two subsets, which have the same "configuration matrix," i.e., the same ordered set of mutual distances. The complexity of calculating this modified generating function is the same as for the ordinary generating function of a convolutional code with the same number of trellis states. Bounds on the performance of some interesting codes are given based upon this method. [This research was supported in part by the Center for Magnetic Recording, Research, University of California, San Diego, La Jolla, CA 92093.]

NOTES

SESSION MA5

ESTIMATION THEORY - APPLICATIONS

ON THE BEARING ESTIMATION OF RADIATING SOURCES BY USING HOUSEHOLDER REFLECTIONS,

H.M. BAYRI and C.C. YEH, Electrical Engineering Department, SUNY, Stony Brook, NY 11794-2350, USA.

Bearing estimation of radiating sources by using orthogonal projections are considered. A projection matrix which has a null space equal to the signal subspace is used to form the search function. We show that such a matrix can be formed by using elementary Householder reflections which reduce the covariance matrix into upper triangular form. The number of sources can be determined from the diagonal elements of the triangular form. The method requires considerably less operations than eigenvalue-eigenvector decomposition. Computer simulations show that with a moderate signal-to-noise ratio (10 dB) two sources separated by less than a standard beam width can be clearly identified. [This work was partially supported by Office of Naval Research grant N00014-85-K0610.]

STATE ESTIMATION IN MULTITARGET TRACKERS USING VARIABLE CORRELATION GATES,

ARIE BERMAN and AMNON HAMMER, State of Israel, Rafael - Armament Development Authority, P.O.B 2250 (88), Haifa 31021, Israel.

The paper presents a performance analysis of Kalman filter estimators in multitarget track-while-scan radars, where variable correlation gate dimensions are determined by filter prediction error covariances. Since multiple targets may appear within the correlation gate, track association is implemented by the nearest-neighbor rule with respect to the predicted track position.

Tracking estimation is performed by means of a second-order Kalman filter, taking into account random maneuvers. Target dynamics are estimated in Cartesian coordinates and filter equations for the three coordinates are assumed to be uncoupled. The measurement noise is composed of a thermal noise and false alarms originating from neighboring targets and clutter (distributed uniformly within the correlation gate).

The variable correlation gate width is determined by the position component of the Kalman filter prediction error covariance matrix and the radar resolution cell. Equations, with respect to state, gain and estimation error covariance updating, are derived. It is shown that steady state estimation errors are smaller than those obtained by Kalman filter estimators using correlation gates of fixed dimension. A simulation example is presented as well.

PROJECTION APPROACH TO BEARING ESTIMATIONS,

CHIEN-CHUNG YEH, Electrical Engineering Department, SUNY, Stony Brook, NY 11794-2350, USA.

Bearing estimation based on the projection approach is discussed. A method is presented which computes a projection matrix by using any M rows of the covariance matrix, where M is the number of radiation sources. This method requires considerably fewer computations than projection techniques using eigenvectors, especially when the number of array elements is much larger than the number of sources. Simulation results are presented also.

ESTIMATION OF THE LINE OF SIGHT VECTOR FOR SPACECRAFT CONTROL LABORATORY EXPERIMENT (SCOLE),

A.C. CHOUDHURY and PETER BOFAH, Department of Electrical Engineering, Howard University, Washington, DC 20059, USA.

The configuration for the Spacecraft Control Laboratory Experiments (SCOLE), as proposed by Taylor and Balakrishnan, consists of a reflector or antenna attached to the space shuttle by a long (130 ft) flexible beam. There are two hinges in the system connecting the beam to the shuttle and the reflector to the beam. The above configuration bears some similarity with the wrap-rib antenna proposed by Lockheed for large space structures. In the above configuration, the line-of-sight (LOS) vector is in the direction of a signal emitted from a point in the cargo bay located 3.75 ft. in front of the base of the beam, and reflected off the center of the reflector in the direction of a distant target.

The design challenge as proposed by Taylor and Balakrishnan is to develop control laws which will enable a rapid slew of the line of sight through 20° and keep it there with a pointing accuracy error of less than .02°. The control laws are also to damp the structural vibrations so as to achieve the pointing error accuracy. The forces needed for the slew are provided by thrusters acting about the principal axes of the shuttle, which produce a maximum torque of 10,000 ft-lb about each axis; and by control forces on the center of the reflector, which have a maximum thrust of 800 lb. Two 10 lb proof-mass actuators are available to be positioned on the beam to regulate the slew maneuver and to damp the vibrations. In addition, there are several accelerometers and rate-gyros mounted on the reflector as well as on the shuttle. Also, the center of the shuttle is measured optically.

The objective of this paper is to discuss the estimation complexities of the system based on the sensor outputs and on existing models. We will start from simple assumptions treating the reflector and the rod as rigid bodies and then extend the discussion to the flexible case.

SESSION MA6

VLSI AND SYSTOLIC ARRAYS

LEAST-SQUARES ESTIMATION ALGORITHMS BY QR DECOMPOSITION METHOD FOR SYSTOLIC ARRAYS,

M.J. CHEN and K. YAO, Electrical Engineering Department, University of California, Los Angeles, CA 90024, USA.

Recursive order and time updating algorithms for least-squares estimation have been proposed by Lee, Morf and Friedlander, and by Shensa. Gentleman and Kung, McWhirter, Ling and Proakis, and Kalson and Yao found various QR decomposition techniques based on a systolic array structure for solving this problem. We first consider the use of Householder orthogonal transformation for systolic *QR* decomposition. We show that for a single row time updating, this approach is identical to the Givens rotation method. Issues involved with multiple row time updating by Householder transformation are considered. Next we propose a new version of the square-root free Givens rotation method, and we show that this modified algorithm has simpler computational complexity than other known fast Givens methods and is still numerically stable. We study the complexities of these known systolic least-squares estimation algorithms by their arithmetical operations and inter-cell communication connections, and provide detailed numerical comparisons under finite word length effects and near singular conditions. Finally, we show that after whitening by Cholesky decomposition, the Kalman filter can be formulated as a square-root information filter followed by a least-squares filter and can be jointly implemented in systolic array form.

IMPLEMENTATION OF THE STACK ALGORITHM BY A SYSTOLIC ARRAY,

C.Y. CHANG and K. YAO, Department of Electrical Engineering, University of California, Los Angeles, CA 90024, USA.

Presently, the stack algorithm is not as popular as the Viterbi or Fano algorithms for convolutional decoding. One primary reason is based on the belief that the stack algorithm requires that all paths in the stack are reordered after each decoding step. That not only takes a long time but also depends on the number of paths in the stack. We show that the operation of stack reordering is redundant in the stack algorithm. In fact, the stack algorithm can be modified so that the key step in the algorithm depends on how to efficiently delete the current best path from the stack and insert new paths into the stack. It is shown that these two operations can be implemented by the the systolic priority queue, a special type of systolic array which is able to complete the deletion of the best path and the insertion of new paths in a fixed and short time duration, no matter how many paths are in the stack. Many new and interesting configurations of systolic priority queues are considered, each of which is suitable for VLSI implementation of the stack algorithm.

FINITE FIELD MULTIPLICATION IN VLSI,

KING F. PANG, Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA.

This paper investigates the area **A**, time **T** and period **P** required for computing multiplications in $\mathbf{GF}(2^n)$ under a grid model for very-large-scale-integrated circuits. Asymptotic bounds will be proved for the complexity metrics **A**, **AT**, $\mathbf{AT}^2$, **AP** and $\mathbf{AP}^2$.

Using the bisection information flow argument, we first prove the lower bounds $\mathbf{A} = \Omega(n)$, $\mathbf{AP} \geq \mathbf{AT} = \Omega(n^{3/2})$ and $\mathbf{AP}^2 \geq \mathbf{AT}^2 = \Omega(n^2)$. This shows that the serial-in, serial-out systolic multiplier of Yeh et al. is area optimal, whereas their parallel-in, parallel-out multiplier is $\mathbf{AP}^2$ optimal. We then describe two multiplier architectures. The first architecture is fast and nearly $\mathbf{AP}^2$ - and $\mathbf{AT}^2$-optimal. However, it has poor **AT** and **AP** performances. Moreover, due to the long wires required in this architecture, it does not seem to be easily implementable. The second architecture, in addition to being $\mathbf{AP}^2$-optimal, has a regular structure, is highly pipelineable and is very amenable to practical implementations. [This work was done while the author was with Information Systems Laboratory, Electrical Engineering Dept., Stanford University, Stanford, CA 94305.]

DECODING RATE 1/n CONVOLUTIONAL CODES IN VLSI,

P.G. GULAK, V.P. ROYCHOWDHURY, and T. KAILATH, Information Systems Laboratory, Department of Electrical Engineering, Stanford University, Stanford, CA 94305, USA.

This paper establishes that area-efficient VLSI circuits for decoding Convolutional Codes can be realized by resorting to a well known interconnection scheme in parallel processing known as the shuffle-exchange network. The strategy deals principally with networks of many simple processors, that reside on a single die, connected to perform the Viterbi Algorithm in a highly parallel way. The concept is shown to apply universally to all rate-$1/n$ convolutional codes including those that are generated by shift register sequences containing simple forms of feedback.

A REED-SOLOMON CODE PROCESSING LSI FOR DIGITAL AUDIO,

KEN ONISHI, KAZUHIRO SUGIYAMA, and YOSHINOBU ISHIDA, Consumer Electronics Development Dept., Mitsubishi Electric Corporation, Nagaokakyo, 617, Japan, TETSUYA YAMAGUCHI, Communication Equipment Works, Mitsubishi Electric Corporation, Amagasaki, 661, Japan, and TOHRU INOUE, Information and Electronics Development Dept., Mitsubishi Electric Corporation, Kamakura, 247, Japan.

The Reed-Solomon code is frequently used for error correcting codes in the field of digital audio. The authors have developed an LSI which executes signal processing of Reed-Solomon codes. In this LSI, the action is controlled by microprograms, an encoder, and a decoder in digital audio which can be performed using time-sharing methods. Moreover, the code length and the minimum code distance are easily changeable, and the various decoding algorithms, for example the Euclid algorithm, Berlekamp algorithms, etc, are available.

In this paper, the authors present the high speed calculation circuit scheme which this LSI adopts to perform real-time encoding and decoding of Reed-Solomon codes in digital audio. This LSI can execute one program step per clock cycle, and a joint addition and multiplication operation within one program step. As one of the applications, the authors present a new method for generating parity check symbols which calculates the syndrome for an encoder that uses check symbols from the middle degrees of a polynomial under the (n,k,d) Reed-Solomon code. Such generation is accomplished by the proposed LSI in a small number of program steps.

NOTES

SESSION MA7

DECENTRALIZED DETECTION

DECENTRALIZED SENSOR SCHEDULING,

DEMOSTHENIS TENEKETZIS and M. ANDERSLAND, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109, USA.

Decentralized observers separately observe and estimate the state trajectory of a stochastic dynamic system. At all times, each observer chooses, based on its past information, to make its current observation using one of a finite number of costly, noisy sensors. The observers do not share observations or estimates, yet the objective is to determine causal sensor scheduling policies, and implicitly estimators, which collectively minimize a performance measure coupling the observers' sensor costs and estimation errors.

We show that the observers' ϵ-optimal sensor scheduling policies are non-randomized, open-loop policies that can be determined by solving a deterministic optimal control problem when: the stochastic dynamic system is linear and Gaussian, the observers' sensors are linear and perturbed by additive white Gaussian noise, the performance measure is a quadratic function coupling the observers' sensor costs and estimation errors.

This problem is an abstraction of a class of decentralized tracking problems in which multiple observers collectively choose sensor scheduling and estimation policies to balance the tradeoffs between minimizing each observer's sensor costs, each observer's tracking error, and the possibility of system-wide systematic tracking error.

HIERARCHICAL ESTIMATION IN CORRELATED NOISE,

SUMIT ROY and RONALD A. ILTIS, Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA 93106, USA.

It has been demonstrated for a decentralized sensor network employing a hierarchical estimation procedure that when the measurement noises at the various sensors are independent and Gaussian, it is possible to reconstruct the optimal global estimate from the local estimates. This is no longer possible in general when the measurement noises are correlated. In Section I of the paper, a specific situation is described in which the measurement noises are correlated and yet the optimal global estimate can be reconstructed from the local estimates. In Section II, the general situation is considered in which the measurement noises are correlated between sensors and it is not possible to reconstruct the global estimate based on the local estimates. For this case, the Best Linear Unbiased Estimator (BLUE) is derived to serve as the fusion rule for the central processor as a sub-optimal combining strategy. This estimator is compared with the case when the central processor combines the local estimates on the incorrect assumption of independence between the sensors and the performance improvement is highlighted.

DISTRIBUTED DETECTION OF SIGNALS PERTURBED BY RANDOM CHANNELS,

Z. CHAIR and PRAMOD K. VARSHNEY, Department of Electrical and Computer Engineering, 111 Link Hall, Syracuse University, Syracuse, NY 13210, USA.

In this paper, distributed detection of signals perturbed by random channels is studied. Optimum decision rules are derived using the Bayesian approach. Examples are presented to illustrate the results. [Supported by RADC Contract F30602-81-C-0169].

AN INFORMATION THEORETIC FORMULATION OF THE DISTRIBUTED DETECTION PROBLEM,

I.Y. HOBALLAH and PRAMOD K. VARSHNEY, Syracuse University, Dept. of Electrical and Computer Engineering, 111 Link Hall, Syracuse, NY 13244-1240, USA.

This paper considers detection with distributed sensors and data fusion which has become an important problem. Distributed detection problem is formulated from an information theoretic standpoint. First, we consider the fully distributed system where local decisions are desired. Optimum decision rules at the individual detectors which minimize equivocation are obtained. Then, we consider the case where local decisions are fed to a data fusion center and a global decision is desired. Optimum fusion rule, which minimizes the information loss is derived. [Supported by RADC contract F30602-81-C-0169.]

A CONTINUOUS-TIME DISTRIBUTED VERSION OF WALD'S SEQUENTIAL HYPOTHESIS TESTING PROBLEM,

ANTHONY LaVIGNA, ARMAND M. MAKOWSKI, and JOHN S. BARAS, Electrical Engineering Department and Systems Research Center, University of Maryland, College Park, MD 20742, USA.

Two decision-makers (DMs) equipped with their own sensors, are faced with the following hypothesis testing problem: Decide between hypothesis H_0 and H_1, where

Under H_1: $d\mathbf{X}_t^i = \mu_i\,dt + \sigma_i\,dW_t^i,\ i = 1,2,$ and Under H_0: $d\mathbf{X}_t^i = \sigma_i\,dW_t^i,\ i = 1,2,$

with $\mu_i \neq 0$ and $\sigma_i \neq 0$, $i = 1,2$, non-random; the noises $\{W_t^1,\ t \geq 0\}$ and $\{W_t^2,\ t \geq 0\}$ are independent Brownian motions. Data is observed continuously in time. The DMs do not communicate; at each instant of time each DM can either declare one of the hypotheses to be true or continue collecting data at some cost. The decisions are selected to minimize a joint cost function with two components: the cost for collecting data and the cost for incorrect decision. This problem was considered first in discrete-time by Teneketzis who showed that the person-by-person optimal strategy was of threshold type for each sensor. Here a similar result is derived by arguments based on well-known facts for the single detector problem. The continuity of the paths of Brownian motion leads to explicit formulae for the joint cost function when the detector policies are of threshold type. This is in sharp contrast with overshoot phenomena that lead in discrete time to the Wald approximations. These formulae reduce the original problem to a mathematical programming problem in four variables over a simple constraint set. [Partially supported by an ONR Fellowship, ONR Grants N00014-84-K-0614 and N00014-83-K-0731, NSF Grants NSFD CDR-85-00108 and ECS-83-51836, and a grant from GM Laboratories.]

SESSION MB1

SOURCE CODING I

FIXED RATE ENCODING OF NONSTATIONARY INFORMATION SOURCES,*

JOHN C. KIEFFER, Mathematics and Statistics Department, University of Missouri-Rolla, Rolla, MO 65401, USA.

An expression is obtained for the optimum distortion theoretically attainable when an information source with finite alphabet is encoded at a fixed rate with respect to a single-letter fidelity criterion. The expression is demonstrated by means of an appropriate coding theorem and converse. This new result generalizes the coding theorem of Shannon for stationary ergodic sources, of Gray-Davisson for stationary nonergodic sources, of Ziv for a source producing a deterministic sequence of symbols, and of Gray-Saadat for asymptotically mean stationary sources. [Work supported by NSF Grant ECS-8501068.]

ON THE AVERAGE CODEWORD LENGTH OF OPTIMAL BINARY CODES FOR EXTENDED SOURCES,

BRUCE L. MONTGOMERY and B.V.K. VIJAY KUMAR, Department of Electrical and Computer Engineering, Carnegie-Mellon University, Pittsburgh, PA 15213, USA.

Although optimal binary source coding using symbol blocks of increasing length must eventually yield a code having average codeword length arbitrarily close to the source entropy, it is known that the sequence of average codeword lengths need not be nonincreasing. The sequence is, however, bounded above by the average codeword length of the source, and certain subsequences must be nondecreasing. In this paper, sufficient conditions are obtained describing sources for which a decrease in average codeword length is achieved when coding pairs of symbols. Also obtained is a sufficient condition specifying sources for which no such decrease is possible. [This work was partially supported by NSF Grant ECS-8411623.]

ON THE GAARDER-SLEPIAN 'TRACKING SYSTEM' CONJECTURE,

ZOLTAN GYORFI, and G. SZEKERES, Technical University of Budapest, Hungary, and G. GABOR, Dalhousie University, Halifax, Nova Scotia, Canada.

The model of recursive source coding plays an important role in building a bridge over the gap between the non-constructive information theory/rate-distortion theory and the set of recursive algorithms applied in communication technology. This model makes it possible to include constraints on the complexity (e.g., memory) of the encoder and the decoder. One of the most important questions on the structure of optimal recursive source coding is whether the optimal encoder-decoder has the equal memory (EM) property, which means that the encoder may have the same memory as the decoder has. We say that the encoder-decoder pair has the quasi-EM property if the encoder has only

*Denotes Long Paper

the memory of the decoder and an independent randomization. In the case of first-order Markov sources we show that for each cost function the per letter distortion of an arbitrary encoder-decoder pair can be achieved by an encoder-decoder with the quasi-EM property.

OPTIMAL REDUCED BINARY MODELS FOR THE GAUSSIAN SOURCE OF FIXED PRECISION NUMBERS,

NICHOLAS WEYLAND and EDWARD PUCKETT, Department of Computer Science, Montana State University, Bozeman, MT 59717, USA.

Optimal reduced, in the sense of minimized expected code length for a fixed memory cost, binary models for the Gaussian source of fixed precision real numbers are presented. These models are used to design noiseless source codes which take into consideration the practical trade-off between minimizing memory cost and expected code length. The source codes are then applied to the problem of lossless data compression of computer files of floating point and fixed point numbers for the case where they are generated by a Gaussian source. It is shown that it is impossible to compress Gaussian floating point numbers beyond 26.24 bits per 32 bit float regardless of the variance. This result is machine dependent but our methods apply to any machine. For Gaussian fixed point numbers with 7 integer and 24 fractional bits of precision, out of a possible $2^{31} - 1$ states in the binary model our algorithm finds that less than 150 are actually needed to describe the source with a loss of information of less than 3.43% from the ideal. [This work was supported by NASA - Ames Research Center, Moffett Field, CA under Interchange Number NCA2-1R470-401.]

SESSION MB2

MAGNETIC RECORDING I

THE MAGNETIC RECORDER AS A COMMUNICATIONS CHANNEL,[+]

JOHN MALLINSON, Director, Center for Magnetic Recording Research, University of California, San Diego, La Jolla, CA 92093, USA.

The basic components of a magnetic recording system will be identified. The functions and structure of the writing head, the magnetizable medium (tape or disk) and the reading head will be discussed. The use of a.c. bias to achieve amplitude linearity at the cost of signal to noise ratio will be explained. For other recorders, where a.c. bias is not used, system linearity is achieved by the use of modulation schemes. Expressions for the output signal power spectrum and the noise power spectrum will be presented.

THE CAPACITY OF A MAGNETIC RECORDING SYSTEM AS A FUNCTION OF TRACK WIDTH,

T. HOWELL, IBM Almaden Research Center, San Jose, CA 95120, USA and E. FEIG, IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA.

The information theoretic capacity of the magnetic recording channel has been the subject of considerable attention recently. Most of this attention has focused on the capacity of a single magnetic track of a given, fixed width. In this paper we allow the recording surface to be divided into an arbitrary number of tracks. The track width is chosen to maximize the total storage capacity. The optimum width depends on the way the signal and noise scale with track width. Under assumptions which are appropriate to some current magnetic recording systems it is shown that the total capacity would be substantially increased by the use of much narrower tracks. This analysis ignores the considerable engineering difficulties in constructing such high track-density systems, but it serves to emphasize the need for work in that direction.

CONSTRAINED CODES FOR DIGITAL MAGNETIC RECORDING CHANNELS,[+]

PAUL H. SIEGEL, IBM Almaden Research Center, K69/802, San Jose, CA 95120-6099, USA.

Digital magnetic recording has motivated a considerable amount of research on the problem of constructing efficient invertible codes from unconstrained data into a constrained system of sequences represented by a discrete noiseless channel. A variety of code construction methods have been developed in an effort to design codes which achieve rates approaching the Shannon capacity and which feature practical encoder/decoder implementations, along with limited error propagation in decoding.

In this tutorial talk, we discuss the construction of codes for the channel constraints which have figured prominently in the development of magnetic recording devices,

[+]Denotes Long Paper

namely run-length-limited (RLL) constraints and spectral null constraints.

We will begin with a review of a typical digital magnetic recording channel, in order to motivate the definition of the RLL and spectral null constraints and to highlight the key issues in code performance evaluation. We then turn to a survey of selected codes of practical interest, and the theoretical methods which underly their construction, including optimal block codes used in magnetic tapes, as well as sequence-state and look-ahead codes found in magnetic and optical disks. We conclude with a discussion of the exciting research avenues and practical code construction possibilities opened up by the recent sliding-block code algorithms of Adler-Coopersmith-Hassner and Karabed-Marcus, which exploit techniques of symbolic dynamics to derive systematic code construction procedures for finite and infinite memory channels. (The paper of Adler-Coopersmith-Hassner received the 1985 Information Theory Group Paper Award).

ON RUN-LENGTH-CODES‡

EPHRAIM ZEHAVI, Qualcomm, San Diego, CA 92121, USA, and JACK KEIL WOLF, Center for Magnetic Recording Research and Dept. of Electrical Engineering and Computer Sciences, University of California, San Diego, La Jolla, and Qualcomm, San Diego, CA 92121, USA.

In this paper we give several new results on binary (d,k) codes. First a new derivation for the capacity of these codes is given. The classical derivation follows from writing a difference equation for the number of sequences of length n satisfying the (d,k) constraint and then solving the difference equation for large n. The new derivation starts by considering the code as the concatenation of phrases, each phrase consisting of a set of zeros followed by a one. The phrases are of minimum length $(d+1)$ and of maximum length $(k+1)$. Then the information rate is derived using some information theoretic inequalities. It is proven that the information rate is maximum when the phrases are statistically independent and chosen in accordance with a specific distribution. Based on this result we compute the spectrum of a (d,k) code. Finally the problem of computing the capacity of the binary symmetric channel under the constraint that the input sequences satisfy the (d,k) constraint is considered. Lower bounds on the capacity of such a channel are derived. [This work was partially suppported by the Center for Magnetic Recording, Research, University of California, San Diego, La Jolla, CA 92093.]

‡Denotes Invited Paper

SESSION MB3

RANDOM PROCESSES I

NON-GAUSSIAN RANDOM FIELD MODELS FOR TELECOMMUNICATIONS, SCATTERING, AND REMOTE SENSING,

DAVID MIDDLETON, 127 East 91st Street, New York, NY 10128, USA.

Two main classes of random space-time field are distinguished here: (I) *ambient fields*, and (II) *scattered fields*. The former are generated by individual, independently emitting sources, the latter, by independent sets of coupled sources. Under broad conditions, both are described by appropriate Poisson processes; these Poisson field models represent among others such physical phenomena as electromagnetic interference (EMI) environments in telecommunications, underwater ambient acoustic noise, reverberation and scattering in the medium and at interfaces, and the scattered fields produced in remote sensing applications.

In this paper the general Jth-order characteristic function of the generic Poisson and quasi-Poisson fields is obtained, and corresponding first- and second-order pfd's of these fields explicitly derived. Analogous results for the associated space-time *sampled* fields, are also calculated, where general sampling arrays are specifically introduced. Extensions of the initial scalar results to vector fields are included. Specific attention to physical applications in telecommunications, scattering, and remote sensing is emphasized. [This work was supported under Contract N00014-84-C-0417 with the Office of Naval Research, Code 1111SP.]

PARAMETER ESTIMATION FOR THE CLASS A MIDDLETON MODEL,

S. ZABIN and H.V. POOR, Coordinated Science Laboratory, University of Illinois, 1101 W. Springfield Avenue, Urbana, IL 61801, USA.

A physically meaningful model for narrowband impulsive interference is the Class A Middleton Model, whose parameters, A and Λ, can be adjusted to fit a great variety of noise phenomena. The quantity A is the "Overlap Index" or "Nonstructure Index," which is a measure of the average overlap of successive emissions, and Λ represents the "Gaussian factor," which relates Gaussian to non-Gaussian components.

We consider several estimators of A and Λ based on channel measurements. Inherent drawbacks of some classical estimators for the A are identified and explained. In particular, traditional likelihood-based estimators may lack consistency. Also, although a consistent, asymptotically normal and asymptotically unbiased estimator is easily established via the method of moments, a performance analysis of this estimator reveals its inefficiency. However, the use of this moment-based estimator as a first approximation in a likelihood-based estimator is seen to lead to a consistent and asymptotically efficient estimator. Similar modifications of earlier heuristic estimators for this model are also considered in a small-sample context. [This work was supported by the Joint Services Electronics Program (U.S. Army, U.S. Navy and U.S. Air Force) under contract N00014-84-C-0149.]

ALMOST SURE CONVERGENCE RATES FOR RECURSIVE PROBABILITY DENSITY ESTIMATORS OF STATIONARY PROCESSES,

ELIAS MASRY, Department of Electrical Engineering and Computer Sciences, University of California at San Diego, La Jolla, CA 92093, USA and LASZLO GYÖRIF, Technical University of Budapest, H-1111 Budapest, Stoczek u.2 Hungary.

Let $\{\underline{X}_j\}_{j=-\infty}^{\infty}$ be a vector-valued stationary process with univariate probability density f on R^d. We consider the recursive estimation of $f(\underline{x})$ from n observations $\{\underline{X}_j\}_{j=1}^{n}$ which need not be independent. For processes $\{\underline{X}_j\}_{j=-\infty}^{\infty}$ which are asymptotically uncorrelated, we establish sharp rates for the almost sure convergence of kernel-type estimations $f_n(\underline{x})$.

A GENERALIZATION OF THE RICE-CRAMER-LEADBETTER LEVEL CROSSING FORMULAS TO HARMONIZABLE PROCESSES,

DANIEL D. CARPENTER, TRW, Redondo Beach, CA, USA and DOUGLAS R. ANDERSON, Independent Consultant, Van Nuys, CA, USA.

This paper presents a generalization of the Rice-Cramer-Leadbetter factorial moment formulas to slope-constrained level crossings of certain harmonizable processes based on a paper previously published by the present authors. Specifically, given a harmonizable Gaussian process with a mean-square derivative satisfying certain continuity conditions, the authors have found Rice-type formulas for all factorial moments of the number of upcrossings of an arbitrary level with the following constraint on the sample function derivative; only those upcrossings of a sample function $X(t)$ are counted which are points of density of the set where $X(t) > a > 0$. These factorial moment formulas permit a generalization to harmonizable processes with slope constraints of Kac and Slepian's horizontal window probability formulas as well as a generalization of the series formulas of Rice and Longuet-Higgins for first passage time probabilities. Previously required assumptions such as sample function derivative continuity or stationarity have been found unnecessary for the new results.

CONDITIONAL LIMIT THEOREMS FOR EMPIRICAL MEASURES AND THEIR MARGINALS,

PAUL ALGOET, Boston University College of Engineering, 110 Cummington Street, Boston, MA 02215, USA

Let M be the distribution of an irreducible Markov process $\{X_i\}_{-\infty<i<\infty}$ with values in a finite set χ. The empirical measure $\hat{P}_n$ is defined as the distribution of the process whose realizations are the n possible shifts of the periodic extension of $X_0, \ldots, X_{n-1}$, and its $(k+1)^{st}$ order marginal $\hat{P}_n(x_0, \ldots, x_k)$ is called the empirical k^{th} order Markov type of the sequence $X_0, \ldots, X_{n-1}$. It is well known that $\hat{P}_n$ converges exponentially fast towards the distribution M of the process $\{X_t\}$, and $\hat{P}_n(x_0, \ldots, x_k)$ converges exponentially fast towards the corresponding marginal $M(x_0, \ldots, x_k)$.

If $\hat{P}_n$ is restricted to a suitable constraint set C then $\hat{P}_n$ converges exponentially fast in conditional probability towards the measure P^* in C that is nearest to M in an information theoretic sense. P^* is the I_M-projection of C, the unique measure in C that attains the minimum relative entropy rate $\inf_{P\in C} I_M(P)$. In particular, if the k^{th} order Markov type $\hat{P}_n(x_0, \ldots, x_k)$ is restricted to a suitable set C then P^* is k^{th} order Markov, and P_n is asymptotically quasi-Markovian with conditional limit P^*.

Similar conclusions hold if the empirical types $\hat{P}_n$ are defined without wrap-around, as empirical distributions of the sliding blocks $\{X\}_{<t} = (\cdots, X_{t-2}, X_{t-1})$.

NOTES

SESSION MB4

OPTICAL COMMUNICATIONS I

BINARY-INTERLEAVED CODING ON THE DEGRADED *M*-ARY PPM DIRECT-DETECTION OPTICAL CHANNEL,‡

G. BECHTEL and J.W. MODESTINO, Electrical, Computer and Systems Engineering Department, Rensselaer Polytechnic Institute, Troy, NY 12180, USA.

The *M*-ary PPM direct-detection optical communication channel in the presence of dark current can be represented as an *M*-ary symmetric erasure channel (MSEC). In this paper a novel binary finite-state channel model for the MSEC is developed. The finite-state model provides an interesting method of viewing the correlation between binary errors and erasures on the MSEC. Under the assumption of full state information about the finite-state model, the capacity and cutoff rate are calculated. These values exceed the standard capacity and cutoff rate of the MSEC, indicating that interleaved binary coding methods utilizing the finite-state model have a potential superiority over standard *M*-ary coding schemes for the degraded direct-detection optical PPM channel. Similar conclusions have been previously provided by Massey for the ideal channel where only erasures but not errors are possible. The finite-state model also points out an interesting and practical coding implementation when perfect state knowledge is unavailable. This implementation utilizes a bank of correlated binary decoders with a provision for transferring information from one decoder to another. This allows the bank of correlated binary decoders to provide superior performance over the same bank of decoders working independently. [This work was supported in part under NAVAIR under Contract No. N00019-83-0-0302 and in part by Caltech under Contract No. PF-233.]

PATTERN CODE MODULATION AND OPTICAL DECODING - A NOVEL CODE DIVISION MULTIPLEXING TECHNIQUE FOR MULTI-FIBER NETWORKS,

JOSEPH Y. HUI, Bell Communications Research, 435 South Street, MRE P-370, Morristown, NJ 07960, USA.

We consider the use of multiple high capacity fibers for communications networking. Each user transmits, asynchronously, patterns of optical pulses distributed over the fibers and throughout a time frame. Each receiver has a distinct alphabet of patterns, which are detected by optical correlators. Optical correlation by fiber tapped delay lines provides speedy and easy-to-implement decoders. Thus the individual user obtains a transparent, low speed channel by code multiplexing. The reliability of this low speed channel can be enhanced by redundantly coding the patterns sent by the user, for which the encoding and decoding processes can be performed electronically. This two-step encoding process is simple to implement, highly reliable at reasonable throughput, and provides asynchronous access with simple protocol. Various components and

‡Denotes Invited Paper

configurations of this access scheme are described. The information theoretic capacity and the error probability for these configurations are derived. We also demonstrate that hardlimiting and filtering at the receiver reduce error probability significantly.

OPTICAL COMMUNICATIONS USING CONSTANT WEIGHT CODES,

GUILLERMO E. ATKIN and IAN F. BLAKE, Department of Electrical Engineering, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada.

Optical communication systems used in space applications have enjoyed an increased popularity over the last few years. Several authors have extensively researched the problem based on the use of a pulse position modulation (PPM) scheme and assuming a noiseless environment. Several options of coding have been proposed evaluating the performance of the system considering the probability of error (or erasure) versus the rate ρ in nats per photon.

In this paper the use of a class of constant weight codes (weight 3) is analyzed and some gains are obtained depending on the parameters under consideration. The relation between probability of error (or erasure), the average number of photons per transmitted pulse (λ), the rate ρ in nats per photon and the rate r in nats per second is examined. It is shown that for $\lambda < \lambda_0$ and with different constraints (energy, bandwidth, average number of photons per second) the performance of the proposed systems depends strongly on the parameters under consideration and the general performance of the systems is a trade-off between the above parameters. For medium and large levels of energy ($\lambda > \lambda_0$) the coded system performs in general better than the PPM system.

EXCESS JITTER ACCUMULATION IN OPTICAL FSK HETERODYNE REGENERATOR CHAINS DUE TO NON-NEGLIGIBLE LASER LINEWIDTH,

MICHAEL J. CARTER, Massachusetts Institute of Technology, Lincoln Laboratory, Lexington, MA 02173-0073, USA.

The accumulation of timing jitter is a principal concern in the design of large digital transmission networks that employ self-timing regenerators. We show that the non-negligible phase noise of semiconductor lasers used in heterodyne optical fiber communication links can appreciably increase the jitter produced in a single regenerator. Furthermore, we show that the accumulation of this excess jitter component in a chain of regenerators can (in several cases of practical interest) dominate the accumulation of systematic jitter. Since most networks are designed with only systematic jitter taken into consideration, these results imply that network performance can be degraded by the presence of the laser phase noise contributed jitter. [This work was sponsored by the Department of the Air Force.]

SESSION MB5

RANDOM ACCESS COMMUNICATIONS I

RANDOM ACCESS COMMUNICATION AND GRAPH ENTROPY,

J. KÖRNER and K. MARTON, Mathematical Institute of the Hungarian Academy of Sciences, Budapest, P.O.B. 127, H-1364, Hungary.

Conflict resolution in random access communication raises the following probabilistic problem. Let $U_1, \ldots, U_k$ be independent random variables uniformly distributed over the unit interval [0,1]. We say that a k-partition A of [0,1] (i.e., a partition into k atoms) separates the (random) points $U_1, \ldots, U_k$ if each atom contains exactly one of the U_i. For k-partitions $A_1, \ldots, A_n$ let $P_{A_1, \ldots, A_n}(k)$ be the probability of the event that at least one of the A_j separates $U_1, \ldots, U_k$. We are interested in the maximum of these probabilities when $A_1, \ldots, A_n$ vary. We exhibit an example that disproves an earlier conjecture by Hajek. We then derive the lower bound

$$1 - P_{A_1,\ldots,A_n}(k) \geq 2^{-n\ k!/k^{k-1}}.$$

The proof is achieved by a new technique for lower bounding teh number of graphs of given structure needed to cover all eduges of a given graph, which in turn is based on the subadditivity of graphy entropy.

THE 'MOVING SERVER' PARADIGM - A UNIFIED APPROACH TO THE DELAY ANALYSIS IN A SURPRISINGLY BROAD CLASS OF RANDOM ACCESS PROTOCOLS,

MART L. MOLLE, Computer Systems Research Institute, University of Toronto, Toronto M5S 1A4, Canada.

In a moving server queueing system, the server walks down the arrival time axis at constant speed, searching for customers. Whenever he encounters one, he pauses to offer service and then resumes his walk. This 'moving server' paradigm of interest for two reasons. First, under fairly general assumptions we can transform a moving server system into a 'synthetic system' - an ordinary queueing system without overhead due to the motion of the server, but with modified customer service times. The delay in the moving server system can easily be obtained from the corresponding result for the synthetic system, providing the latter system can be solved. Second, it allows us to model the delay in a broad class of random access protocols in which the selection of packets for transmission resembles a 'sliding window'. These include Virtual Time CSMA (with and without Head-of-the-Line priority classes), a novel hybrid CSMA/binary search group testing protocol (that takes advantage of the cheap something/nothing feedback implied by carrier sensing), a windowed version of Capetanakis' Tree Conflict Resolution Algorithm, and even a 'helical window' token ring. We note that in the case of the last two protocols, our method gives *exact* results.

ERASURE, CAPTURE AND RANDOM POWER SELECTION IN MULTIPLE-ACCESS SYSTEMS,

ISRAEL CIDON, HAREL KODESH, and MOSHE SIDI, Department of Electrical Engineering, Technion - Israel Institute of Technology, Haifa, Israel.

A communication system with many nodes accessing a common receiver through a time-slotted shared radio channel, is considered. Ideally, each transmission of a node is heard by the receiver. In practice, however, due to topological and environmental conditions, the receiver is prone to fail to hear some or all of the packets transmitted in a slot. The phenomena of failing to detect *any* packet is called **erasure**, while detecting a *single* transmission out of many is called **capture**.

This paper introduces multiple access algorithms that handle erasures as well as captures. The algorithms are evaluated according to the maximal throughput that they can support for Poisson arrival process. An example is given that shows that, in practice, the positive effect of captures compensates the negative effect of erasures. In addition, we introduce a new approach to effectively exploit the capture phenomena. This approach incorporates a random power selection scheme that allows each node to randomly choose to transmit in one of several allowable levels of power. Design issues such as number of levels, selection schemes etc. are discussed.

PERFORMANCE EVALUATION OF INTERVAL-SEARCHING CONFLICT RESOLUTION ALGORITHMS,

WOJCIECH SZPANKOWSKI, Department of Computer Science, Purdue University, West Lafayette, IN 47907, USA.

A single multiaccess channel is studied with the outcome of a transmission being either "idle", "success", or "collision" (ternary channel). Packets involved in a collision must be retransmitted, an efficient way to resolve collisions being the Gallager-Tsybakov-Mikhailov (GTM) algorithm. Performance analysis of the algorithm was based on a numerical solutions,that fail to provide insight into the behavior of the algorithm. We shall present a new look at the algorithms and discuss some attempts of analyzing its performance. In particular, expected lengths of a resolved interval and a conflict resolution interval as well as throughput of the algorithm will be discussed using asymptotic approximation and "a small input rate" approximation. We shall show that for GTM algorithm the average time to solve a conflict of multiplicity n is $O(lg\ n)$, and the average length of resolved interval is $O(n^{-1})$. However, to determine throughput of the algorithm we must estimate not only the average values of conflict resolution interval and resolved interval, but we need a tight approximation for generating functions for the above quantities. This is done through so called *small input rate approximation*. We shall show that the real throughput equal 0.48771 is approximated by 0.48819 in the small input rate approximation. Finally, we generalize these results to cover a wider class of interval-searching algorithms.

AN IMPROVED UPPER BOUND ON CAPACITY OF THE RANDOM MULTIPLE-ACCESS CHANNEL,

B.S. TSYBAKOV and N.B. LIKHANOV, Institute for Problems of Information Transmission, U.S.S.R. Academy of Science, 19 Ermolovy St., USSR-101447, Moscow GSP-4, U.S.S.R.

The capacity, C, of the slotted random multiple-access (RMA) channel is the supremum of the throughputs of all algorithms for servicing the traffic, which is assumed to be Poisson and to be generated by infinitely many identical users, with the aid of noiseless ternary feedback (idle, success, collision). Pippenger obtained the first upper bound on C, $C \leq 0.744$. Molle showed that $C \leq 0.673$. Cruz and Hajek proved that $C \leq 0.612$. Mikhailov and Tsybakov obtained the bound $C \leq 0.587$ that was sharpened by Zhang and Berger to $C \leq 0.578$. In the present paper, the bound $C \leq 0.568$ is established. The reader is reminded that the best lower bound on C is the achieved throughput of the part-and-try algorithm, namely 0.487.

NOTES

SESSION MB6

ALGEBRAIC CODING THEORY I

Q-CODES,[+]

VERA PLESS, Mathematics Department, University of Illinois at Chicago, Chicago, IL 60680, USA.

We introduce a new, infinite family of $(n, \frac{n+1}{2})$ and $(n, \frac{n-1}{2})$ codes over $GF(4)$. These include Q.R. codes when n is prime. These codes, called Q-codes, are defined in terms of their idempotent generators and exist for all odd n. The idempotent generators can be easily constructed, even for large n, from the quaternary cyclotomic cosets without factoring x^n-1.

All self-dual (s.d.) and strictly self-dual (s.s.d.) extended cyclic quaternary codes are extended Q-codes. We can tell by the factors of n whether s.d. or s.s.d. quaternary codes of length $n+1$ exist. We know at which lengths Q-codes have binary idempotents or when the binary subcode is the all-one vector.

A square-root bound holds for the minimum odd-like weight of vector in a Q-code. Conditions are given under which the supports of the minimum weight vectors in a Q-code hold a projective plane. A cyclic projective plane of order 2^s is contained in a cyclic quaternary code whose extension is s.s.d. iff either s is odd or is $\equiv 2 \pmod 4$. [The work was partially supported by NSF Grants MCS-8201311 and R11-8503096 and NSA Grant MDA 904-85-H-0016.]

SELF-DUAL CODES OVER *GF(7)*,

VERA PLESS, Mathematics Department, University of Illinois, Chicago, IL, USA and VLADIMIR D. TONCHEV, Institute of Mathematics, Bulgarian Academy of Sciences, Sofia, Bulgaria.

We have completely classified all maximal self-orthogonal codes of lengths 3,5,6,7 and 9 over $GF(7)$ and all self-dual codes of lengths 4 and 8 over $GF(7)$. We give a canonical basis for each code, its Hamming weight distribution and the order of its monomial group. There are 20 inequivalent (9,4) self-orthogonal codes over $GF(7)$, 15 of which are indecomposable. In order to do this, we give formulas for the number of maximal self-orthogonal codes over $GF(7)$ of length n when n is either odd or $\equiv 2 \pmod 4$ and for the number of self-dual codes over $GF(7)$ when $n \equiv 0 (mod\ 4)$. We also give formulas to count the number of self-dual or maximal self-orthogonal codes of length n containing a self-orthogonal subcode C where the number of containments of codes equivalent to C are counted.

From this classification it follows that the known M.D.S. codes over $GF(7)$ of length 6,7 and 8 are the unique maximal self-orthogonal or self-dual M.D.S. codes (over $GF(7)$) of these lengths. They are all cyclic.

[+]Denotes Long Paper

HASSE DERIVATIVES AND REPEATED-ROOT CYCLIC CODES,

JAMES L. MASSEY, NIKI VON SEEMAN, and PHILIPP SCHOELLER, Institute for Signal and Information Processing, Swiss Federal Institute of Technology, CH-8092 Zurich, Switzerland.

A derivative, introduced by H. Hasse fifty years ago, is shown to be the natural tool for the study of repeated-root cyclic codes, i.e., cyclic codes whose generator polynomial $g(X)$ has at least one root of multiplicity greater than 1. The n^{th} Hasse derivative of the polynomial $a(X) = \sum_i a_i X^i$ is defined as $a^{[n]}(X) = \sum_i \binom{i}{n} a_i X^{i-n}$, and hence is related to the n^{th} formal derivative $a^{(n)}(X)$ by $a^{(n)}(X) = n!\, a^{[n]}(X)$. The Hasse derivative has the property that $[M(X)]^e$, where $m(X)$ is irreducible with $m^{(1)}(X) \neq 0$, divides $a(X)$ if and only if $m(X)$ divides $a(X)$ and its first $e - 1$ Hasse derivatives.

The Hasse derivative is used to specify the parity-check matrix of a repeated-root cyclic code of length N. It is shown that if α is a root of $g(X)$ with multiplicity e, then the N-tuple

$$\left[\binom{N-1}{i}\alpha^{N-1}, \binom{N-2}{i}\alpha^{N-2}, \ldots, \binom{0}{i}\right]$$

is in the dual code for $i = 0,1,\ldots,e-1$.

The Hasse derivative is also exploited to determine the minimum distance of binary repeated-root cyclic codes, i.e., binary cyclic codes with even length N. The minimum distance is shown to be the minimum of the minimum distances of a specific set of binary cyclic codes of odd length n, the largest odd divisor of N, specified by the multiplicities of the roots of $g(X)$. This result is used to compile a list of binary repeated-root cyclic codes that are as good as the best known codes with the same length and rate, or nearly as good.

NEW CODES FROM ALGEBRAIC CURVES OF GENUS 2,

S. HARARI, Groupe d'Etude du Codage de Toulon, Université de Toulon et du Var, Avenue de l'Université, 83130 La Garde, France.

It is known that Reed Solomon codes, and B.C.H. codes can be obtained as codes on algebraic curves of genus 1. In this work we apply desingularization techniques to curves of genus 2 to obtain curves with a large number of rational points over a prime field F_p. We start with a curve having singularities and find a model with all the singularities removed and changed into rational points. This is a bounded recursive process which ends with a curve having no singularities and a large number of rational points. These resulting curves are applied to some well known techniques to find the associated codes. We study their length and dimension. We attempt to find their minimum weight using a special algorithm and a decoding algorithm using a known algorithm [Harari, S., *IEEE ISIT,* Brighton, June 1985]. We also give a complexity estimate of the code construction.

SESSION MC1

CODING I

A NEW APPROACH TO THE COVERING RADIUS OF CODES,[1]

N.J.A. SLOANE, Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974, USA.

We introduce a new approach which facilitates the calculation of the covering radius of a binary linear code. It is based on determining the *normalized covering radius* ρ. For codes of fixed dimension we give upper and lower bounds on ρ that are reasonably close. As an application, an explicit formula is given for the covering radius of an arbitrary code of dimension ≤ 4. This approach also sheds light on whether or not a code is normal. All codes of dimension ≤ 4 are shown to be normal, and an upper bound is given for the norm of an arbitrary code. This approach also leads to an amusing generalization of the Berlekamp-Gale switching game.

ON THE COVERING RADIUS OF LONG BINARY BCH CODES,

A. TIETÄVÄINEN, Department of Mathematics, University of Turku, SF-20500 Turku, Finland.

Tor Helleseth showed that equations over finite fields can be related to certain problems in the theory of codes. In particular, he proved that the covering radius of any long binary BCH code with designed distance $2t + 1$ is at least $2t - 1$ and at most $2t + 1$. Now we close this gap halfway by showing that the covering radius is at most $2t$ if the word length is sufficiently large, and consider also some other connections between character sums, codes, and equations over finite fields.

THE COVERING RADII AND NORMALITY OF t-DENSE CODES,

H. JANWA and H.F. MATTSON, School of Computer and Information Science, Syracuse University, Syracuse, NY 13244-1240, USA.

We introduce t-density for codes to find either the exact value of or an upper bound on the covering radii of index-2 subcodes. Results on the number of cosets of maximum weight of such codes are also given. Exact results on the event subcodes are obtained for, among others, s-error-correcting BCH codes (s=2,3), and punctured RM codes (of order m-3). Exact covering radii of shortened codes are determined for some of the above codes, proving that some of the codes are normal. Improved upper bounds on the norms of t-dense codes are also given.

[1]Denotes Long Paper

NOTES

SESSION MC2

MAGNETIC RECORDING II

BINARY CONVOLUTIONAL CODES WITH APPLICATION TO MAGNETIC RECORDING,[+]

A.R. CALDERBANK, Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974, USA, and CHRIS HEEGARD and T.-A. LEE, School of Electrical Engineering, Cornell University, Ithaca, NY 14853, USA.

Calderbank, Heegard, and Ozarow have suggested a method of designing codes for channels with intersymbol interference, such as the magnetic recording channel. These codes are designed to exploit intersymbol interference. The standard method is to minimize intersymbol interference by constraining the input to the channel using run-length limited sequences. Calderbank, Heegard, and Ozarow considered an idealized model of the magnetic recording channel that leads to the problem of designing codes for a partial response channel with transfer function $(1 - D^N)/2$, where the channel inputs are constrained to be ± 1. This is the problem we consider here. Channel inputs are generated using a non-trivial coset of a binary convolutional code. The coset is chosen to limit the zero-run length of the output of the channel and so maintain clock synchronization. The minimum squared Euclidean distance between outputs corresponding to distinct inputs is bounded below by the free distance of a second convolutional code which we call the magnitude code. An interesting feature of the analysis is that magnitude codes that are catastrophic may perform better than those that are non-catastrophic. [This research was supported by NSF Grant ECS 8353330 and by IBM under the Faculty Development Award program.]

CROSS PARITY CHECK CONVOLUTIONAL CODES FOR MAGNETIC TAPE,

TOM FUJA, CHRIS HEEGARD, School of Electrical Engineering, Cornell University, Ithaca, NY 14853, USA, and MARIO BLAUM, IBM Almaden Research Center, 650 Harry Road, San Jose, CA 91520, USA.

In this paper we define and analyze *cross parity check* (CPC) convolutional codes, a class of error-control codes with both interesting theoretical properties and practical implementation advantages. CPC codes evolved from ideas used in an error-control scheme implemented on the IBM 3480 tape sub-system.

In this paper, we begin by placing both the 3480 code and its variation in a firm convolutional code context; specifically, we construct parity check matrices and describe systematic generators for these codes. Having done so, we use the insight gained to define the class of CPC codes and to construct canonical parity check and generator matrices. We then prove that CPC codes — unlike the IBM 3480 code — are, in fact, maximum

[+]Denotes Long Paper

distance separable (MDS) convolutional codes, as defined by P.Piret and T. Krol. Next, we demonstrate how CPC encoding/decoding delay can be shortened by "folding" the parity check lines by dividing each term in the parity check matrix by some fixed polynomial, keeping only the remainder. In particular, we give a class of polynomials that, when used in this way, produce a code that is not only still MDS, but also retains much of its geometrical regularity. Finally, we finish by giving some general error-erasure decoding algorithms for CPC codes. [This work has been supported by NSF Grant ECS-8352220, by an IBM Faculty Development Award, and by the AT&T Bell Laboratories Ph.D. Scholarship program.]

SLIDING-BLOCK CODING FOR INPUT-RESTRICTED CHANNELS,

RAZMIK KARABED and BRIAN MARCUS, IBM Almaden Research Center K69/802, 650 Harry Road, San Jose, CA 95120, USA.

We continue here the work of Adler, Coopersmith, and Hassner (see IEEE-IT 29, 5-22) and Marcus (see IEEE-IT 31, 366-377) on coding arbitrary sequences into a constrained system of sequences (called a sofic system). Such systems model the input constraints for input-restricted channels (e.g., run-length limits and spectral constraints for the magnetic recording channel). In this context, it is important that the code be non-catastrophic; for then the decoder will have limited error propagation. We give a constructive proof of the existence of finite-state, invertible, non-catastrophic codes from arbitrary n-ary sequences to a sofic system S at constant rate p:q provided only that Shannon's condition:

$$(p/q) \leq (C/\log n) \qquad (*)$$

is satisfied (here C is the capacity of the system S). If strict inequality in (*) holds or if equality in (*) holds and S satisfies a natural condition, called "almost of finite type" (which includes the systems used in practice), we get a stronger result: namely, the decoders can be made "state-independent" sliding-block. This generalizes the results of Adler, et. al., and Marcus. We also give an example to show that the stronger result does not hold for general sofic systems.

A LINEAR BOUND FOR SLIDING-BLOCK DECODER WINDOW SIZE,

JONATHAN ASHLEY, IBM Almaden Research Center K69/802, 650 Harry Rd., San Jose, CA 95120, and Computer and Information Sciences Board, University of California, Santa Cruz, CA 95064, USA.

Adler, Coopersmith, and Hassner (see IEEE-IT 29, 5-22) present methods for coding arbitrary n-ary sequences into constrained systems of sequences, called subshifts of finite type, defined by labeled directed graphs. An example is the run-length limited system for the magnetic recording channel. Their codes have limited error propagation because the decoders are sliding-block with a finite window size. We prove an upper bound for the necessary decoding window size. For codes, with coding ratio 1, from arbitrary n-ary sequences into subshifts of finite type of entropy at least $\log(n)$, where n is an integer, the bound is quadratic in the number of states in the natural directed graph defining the constrained system of sequences. In case the entropy is greater than $\log(n)$ and the memory of the subshift of finite type is 1, the bound is linear.

SESSION MC3

SPEECH AND IMAGE PROCESSING

A SEGMENT MODEL FOR PHONETIC RECOGNITION OF CONTINUOUS SPEECH,

MARI OSTENDORF DUNHAM and S. ROUCOS, BBN Laboratories, Cambridge, MA 02238, USA.

We present a new approach to the recognition of phonemes in continuous speech which uses a joint model of all parameters representing the segment of speech that corresponds to a phoneme. This phoneme segment is a variable-length sequence of feature vectors that is transformed into a fixed-length sequence by a time-warping algorithm. Given the phonetic segmentation of an utterance, we recognize the sequence of phonemes by either minimum distance or maximum likelihood classification methods. When the phonetic segmentation is unknown (as would be the case in speech recognition), the utterance can be jointly segmented and recognized by using a dynamic programming algorithm. We will describe the segment model approach to phoneme recognition, present performance results for minimum distance and maximum likelihood pattern matching approaches to recognition of hand-segmented speech, and give phoneme recognition results using the automatic segmentation algorithm.

ON OPTIMAL IMAGE DIGITIZATION,

A.M. BRUCKSTEIN, Department of Electrical Engineering, Technion, Israel Institute of Technology, Haifa, 32000, Israel.

Neilsen, Astrom and Jury recently addressed the problem of determining the optimal discretization grid and quantization depth when a given bivariate function $f(x,y)$ has to be described with a predetermined number of bits. This was done under the assumption that the function value range and mean "fluctuation rates" in the x and y direction are given and that ideal point sampling with zero-order-hold interpolation is used in reconstructing the image. This note outlines an alternative approach, based on the assumption that $f(x,y)$ is the sample function of a 2-D stationary stochastic process with a known covariance function. We use standard integral sampling and obtain closed form solutions under the assumption that $f(x,y)$ is (the sample of) a homogeneous and separable Markov process.

SUBPIXEL ACCURACY OF DIGITIZED BILEVEL PICTURES,

JACK KOPLOWITZ and A.P. SUNDAR RAJ, Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13676, USA.

Bilevel pictures are generally digitized using a grid of square cells, with side T, which are colored either black or white. We consider the case where the cell or pixel level is determined by whether the center point of the cell lies in the black or white region of the

image. If the boundary of the silhouette can be assumed to be straight within a cell, this procedure is equivalent to assigning the level closest to the average within a digitizing cell. The resulting digitized silhouette consists of regions whose boundaries are links of horizontal and vertical line segments of length T.

BACKWARD ADAPTIVE TREE ENCODING OF LINE DRAWINGS,

M. VEMBAR and S. MOHAN, Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY 13767, USA.

Chain codes belong to the line-following type of encoding techniques which are used to encode or digitize line drawings. Different chain coding schemes exist such as the square quantization and grid intersect quantization methods. We use the simplest search algorithm, the single path algorithm (DPCM) to encode line drawings to form a basis for comparison of other schemes. Tree coding schemes are used to encode random curves whose tangents at sample points along the curve form an autoregressive process. The (M-1) algorithm performs 2.34 dB (with a code rate of 1 bit/sample) and 2.36 dB (with a code rate of 2 bits/sample) better than DPCM. When the code tree is smoothed by a rate-distortion-derived filter for autoregressive sources, performance improves to 3.8 dB (1 bit/sample) and 3.809 dB for 2 bits/sample).

The introduction of an adaptive quantizer and an adaptive predictor results in even better performance. We first used an adaptive gradient algorithm to adapt the tree code and used the (M-1) Algorithm to search the tree. We obtained an improvement of 3.91 dB (1 bit/sample) and 4.3 dB (2 bits/sample) over DPCM. Tree encoding using the backward adaptive Kalman filter improved the performance even further -- a gain of 3.94 dB (1 bit/sample) and 4.54 dB (2 bits/sample).

EDGE PRESERVING IMAGE RESTORATION WITH ROBUST IMAGE MODELLING TECHNIQUES,

KIE-BUM EOM and R.L. KASHYAP, School of Electrical Engineering, Purdue University, West Lafayette, IN 47907, USA.

Traditionally, median filters or α-trimmed mean filters are used to restore images that are contaminated by impulse noise. However, these approaches may also blur images. Since they are based on the assumption of constant image intensity within a window. An image model approach is used in this blurring problem. The image intensity function in a window is assumed to follow a three-neighbor causal autoregressive model. The parameters of the model are estimated by robust M-estimator regression through iterative application of a least squares algorithm and a data-cleaning procedure using a 3-σ rule. As the estimated parameter converges to the robust M-estimator, *impulsive* noise in the original image will be significantly reduced. Therefore, the resulting image is restored from impulsive noises. The performance of the robust model based restoration algorithm is compared with that of the median filter for two different real images. The experimental result shows that the robust model based approach performs better than the median filter approach. The iterative method converges only after 3 iterations in our experiment. [Partially supported by the Office of Naval Research under the grant N00014-85K-0611 and by the National Science Foundation under the grant IST-8405052.]

SESSION MC4

COMMUNICATION SYSTEMS

CROSS-POLARIZATION CANCELLATION AND EQUALIZATION IN DIGITAL TRANSMISSION OVER DUALLY POLARIZED MULTIPATH FADING CHANNELS,*

M. KAVEHRAD and J. SALZ, AT&T Bell Laboratories, Inc., Crawford Hill, Holmdel, NJ 07733, USA.

A theory for data-aided equalization and cancellation in digital data transmission over dually polarized fading radio channels is presented. The present theory generalizes and extends previous work by admitting decision feedback structures with finite-tap transversal filter implementations. Subject to the assumption that some past and/or future data symbols are correctly detected, formulas and algorithms for evaluating the least mean-square error for different structures are presented. In a sequence of curves we evaluate and compare the performance of various structures for a particular propagation model and several fading events. We discover that decision feedback/canceler structures are much less sensitive to timing phase than linear equalizers. There is, however, a caveat associated with the advantages of decision feedback/canceler structures over linear equalizers. These nonlinear techniques can suffer from error propagation, and further work must be done to assess the degree of this penalty. Some experience with these systems in voiceband data transmission indicates that error propagation is not an insurmountable problem and can be essentially disregarded when the precancellation error rate is equal to or better than 10^{-2}. In the present application, the inclusion of this effect in the analysis was found to be mathematically intractable.

SOME LINK JAMMING GAMES,

WEI-CHUNG PENG, ROBERT A. SCHOLTZ, and LLOYD R. WELCH, Communication Sciences Institute, University of Southern California, Los Angeles, CA 90089-0272, USA.

Link jamming problems are formulated as two-person zero-sum infinite games under the following assumptions: (1) the communicator can randomize its power level and/or data rate, (2) the jammer can randomize its power level, (3) both the communicator and the jammer are subject to average (and peak) power constraints P,J (P_{max},J_{max}) respectively, (4) a threshold model for the success of packet transmissions, (5) throughput as the pay-off function. A memoryless model and a generalized model are presented. The optimal memoryless strategies are proven to remain optimal in the generalized formulation.

Link jamming games with average (and peak) power constraints are then analyzed and saddlepoint throughput values are obtained. When only average power constraints are assumed, it is demonstrated that, from the communicator's point of view, (1) power randomization outperforms rate randomization and (2) power and rate randomization do not

*Denotes Long Paper

result in any improvement over pure power randomization. With peak and average power constraints, the above results remain true when $P_{max} \geq J_{max}$. When $J_{max} > P_{max}$, rate randomization may be helpful. [This work was supported by ARO under grants DAAG29-82-k-0142 and DAAG29-85-k-0116.]

SOLUTIONS TO SOME STOCHASTIC TEAM PROBLEMS AND ZERO-SUM GAMES WITH NONCLASSICAL INFORMATION ARISING IN COMMUNICATION SYSTEMS,

RAJESH BANSAL and TAMER BAŞAR, Coordinated Science Laboratory, University of Illinois, 1101 W. Springfield Avenue, Urbana, IL 61801, USA.

Stochastic dynamic optimization problems are said to be of the *nonclassical information* type if (roughly speaking) not all the relevant information acquired and used at earlier stages is available at future stages. Such problems are in general very difficult to solve, both analytically and numerically, and very few closed-form solutions exist in the literature.

In this paper, we will carve out a subclass of such problems, arising in communications, which admit closed-form solutions. We will consider problems with complete statistical description as well as those with incomplete statistical description, with the latter class arising as jamming problems in communications. For these jamming problems we seek closed-form saddle-point solutions in pure or mixed strategies. Some numerical work will complement the theoretical findings.

STOCHASTIC MODEL OF THE PHASE PROCESS IN FM RECEIVERS,

L.L. CAMPBELL, G.D. SWANSON, and P.H. WITTKE, Queen's University, Kingston, Ontario K7L 3N6 Canada.

Let the input to an FM receiver consisting of a limiter, discriminator and integrate-and-dump filter be

$$S(t) = P\cos\omega_0 t + a(t)\cos\omega_0 t - b(t)\sin\omega_0 t \quad ,$$

where P is the signal amplitude and $a(t)$ and $b(t)$ are narrow-band Gaussian processes. The output of the receiver then is $\phi(T) = \int_0^T \dot{\psi}(t)dt$, where ψ is the phase of the input signal and $\phi(T)$ is not reduced modulo 2π. This paper is concerned with both analytic and computer simulation approaches to the determination of the probability distribution of $\phi(T)$.

Our approach is to model $a(t)$ and $b(t)$ as independent Ornstein-Uhlenbeck processes and to write a Fokker-Planck equation for the distribution of amplitude and phase. We obtain a solution involving one infinite integral for the case $P=0$. We also show that $\phi(T)$ has approximately a Cauchy distribution in this case. Analytic results are presented for $P \neq 0$, as well. In addition, distributions have been obtained by computer simulation. [This research was supported by NSERC of Canada research grants to the first and third authors. Part of the work of the first author was performed at the Statistical Laboratory, University of Cambridge and at the Center for Stochastic Processes, University of North Carolina at Chapel Hill. The second author is currently with Bell Northern Research Ltd., Ottawa, Canada.]

SESSION MC5

BLOCK DECODING

FAST SOFT DECISION DECODING OF CYCLIC CODES,

WANG XIN MEI, Department of Information Engineering Northwest, Telecommunication Engineering Institute, Xi'an, The People's Republic of China.

Two decoding algorithms are suggested in this paper. One is the generalized threshold Chase algorithms called GTCI, GTCII, and STC, another is the Chase algorithms in combination with fast soft decision error trap decoding called CFSETD, which is a soft decision decoding with only a simple hard decision decoder. The fundamentals and decoding speed of these algorithms are discussed. The decoding speed of these algorithms is faster then standard Chase algorithms and the probability of decoding error is almost the same as the Chase algorithms. At last, we compare by computer simulations the performance of the threshold Chase algorithms and standard Chase algorithms.

A GENERAL MINIMUM DISTANCE DECODING PROCEDURE FOR BINARY LINEAR BLOCK CODES,

B.L. MONTGOMERY and B.V.K.V. KUMAR, Department of Electrical and Computer Engineering, Carnegie-Mellon University, Pittsburgh, PA 15213, USA and H. DIAMOND, Department of Mathematics, West Virginia University, Morgantown, WV 26506, USA.

We investigate the complexity of a general minimum distance decoding procedure for binary linear block codes used to transmit information over a binary symmetric channel. The procedure involves coset search, and derives its efficiency by exploiting the well-known properties of the code space and the dual code space. The complexity is compared with that of another such procedure, the zero-neighbors algorithm (ZNA). It is shown that for practical values of block error probability and decoding effort, the proposed procedure performs much more efficiently, although the ZNA asymptotic complexity is lower. [This work was partially supported by NSF Grant ECE-8411623.]

A DECODING TECHNIQUE FOR TWICE REED-SOLOMON CODING BASED ON CROSS-INTERLEAVING,

XING DING-JIA and YAO MING-YU, Department of Computer Science, Fudam University, The People's Republic of China.

An interleaving technique with twice Reed-Solomon coding called cross-interleaved Reed-Solomon code (CIRC), abbreviated $RS_1 \times RS_2$, may obtain a low error-rate for random error correction and has powerful potential for burst error correction. Therefore, it is suitable for use as an error-control code in a large capacity, high density data storage device such as an optical disk. In this paper, we will provide an efficient method for

decoding $RS_1 \times RS_2$, i.e., for RS_1 and RS_2 in $RS_1 \times RS_2$ respectively. Compared with some currently available methods, advantages in increasing decoding speed and reducing implementation complexity are obtained. [This work was supported by NSF Grant Tech.-85226.]

ENCODING AND DECODING OF BCH CODES USING LIGHT AND SHORT CODEWORDS,

RON M. ROTH, Department of Computer Science, Technion, Israel Institute of Technology, Haifa 32000 Israel, and GADIEL SEROUSSI, Cyclotomics Inc., 2120 Haste St., Berkeley, CA 94618; on leave from the Department of Computer Science, Technion, Israel Institute of Technology, Haifa 32000 Israel.

It is shown that every q-ary primitive BCH code of designed distance δ and sufficiently large length n contains a codeword c_o of weight $w = O(\delta)$, and degree $\deg(c_o) = o(n)$. We use these light and short codewords to describe an encoding-decoding algorithm which runs on a sequential machine in time $O(\delta n)$. For "small" (e.g., fixed) δ, this is faster than the commonly used algorithms, when run on sequential machines.

GROUPS, FINITE TRANSFORMS AND THE DECODING OF CYCLIC CODES,

R.M. CAMPELLO DE SOUZA, Coordenacao do Mestrado em. Eng. Electrica, Departamento de Eletronica e Sistemas - CT - UFPE, Cidade Universitatia, 50000 Recife - PE Brazil and M.M. CAMPELLO DE SOUZA, Empresa Brasileira de Telecommunicacoes, EMBRATEL, Av. Agamenon Magalhaes 1141, PQE. AMORIM, 50000 Recife PE Brazil.

Decoding methods for error control codes which are based on syndrome look-up tables are of limited use due to the rapidly increasing amount of storage that they require as the number of parity digits of the code increases. By considering the relationship between the finite field Fourier transform and some families of finite groups, we provide an efficient method for partitioning the set of all syndromes of a linear code into equivalence classes. These classes can be counted by the Polya-Burnside method and we show that great reductions in storage requirements are possible, with little increase in decoding complexity. The technique presented can be described as a general type of permutation decoding which makes use of information from the transform domain. [This work was partially supported by Conselho Macional de Desenvolvimento Cientifico e Tecnologico (CNPq).]

SESSION MC6

SHANNON THEORY I

ASYMPTOTIC BOUNDS FOR DISJUNCTIVE CODES,

THOMAS ERICSON, Department of Electrical Engineering, Linkoping University, S-581 83 Linkoping, Sweden.

Disjunctive codes play a fundamental role in multiple access communication in various collision channels. The basic ideas were outlined by Kautz-Singleton, 1964 and further developed by Bassalygo, 1975 and Kyachkov-Rykov, 1982.

A binary code C of length n and size $|C| = T$ is a disjunctive code of order m if the super-position (Boolean sum) of any m codewords does not cover any other codeword in C. Hence, a receiver observing only the Boolean sum is always able to identify the set of codewords forming the sum.

Let $N(m,T)$ be the smallest wordlength n for which a disjunctive code with parameters m,T can be constructed. By an algebraic construction employing the Varshamov-Gilbert bound we prove that $N(m,T)$ is upper bounded by

$$N(m,T) \lesssim N \min\{m^2 \frac{e}{\log e} \log T,\ T\}$$

(The same result was obtained by Dyachkov-Rykov, 1981 with the aid of a random coding argument.)

MULTIPLE DESCRIPTION SOURCE CODING WITH EXCESS RATE,

ZHEN ZHANG, Mathematics Department, Bielefeld University, Bielefeld, West Germany, and TOBY BERGER, School of Electrical Engineering and Center for Applied Mathematics, Cornell University, Ithaca, NY 14853, USA.

Let R_1 and R_2 be the encoding rates of two descriptions of the memoryless source $\underset{\sim}{X} = \{X_k\}$. Let d_i denote the expected per letter distortion between X and $\hat{X}_i$, where $\hat{X}_{i,k}$ is the reconstruction of X_k based solely on the encoding that has rate R_i, i = 1,2. Let d_0 denote the expected per letter distortion between X and $\hat{X}_0$, where $\hat{X}_{0,k}$ is the reconstruction of X_k based on both encodings. Ahlswede has posed the question, "If $R_i = R(d_i)$ for $i = 1,2$, then how small can d_0 be made?" Let us denote this minimum value by $d_0(d_1,d_2)$. In this paper we provide a lower bound to $d_0(d_1,d_2)$. [This work was partially supported by NSF Grant ECS-8305681.]

THE UNINFORMED INTELLIGENT JAMMING CHANNEL,

CHARLES R. BAKER and I.F. CHAO, Department of Statistics, University of North Carolina, Chapel Hill, NC 27514, USA.

We consider the jamming channel where the original additive noise is Gaussian and the jammer adds noise independent of the ambient noise and of the transmitted signal. The channel is without feedback. The constraint on the transmitted signal is a generalized average power constraint given in terms of the original channel noise. The constraint on the jammer is a pure energy constraint. Average mutual information is to be maximized by the coder, minimized by the jammer. A saddle point solution is obtained, i.e., a solution that is simultaneously optimum for both coder and jammer.

COUNTING IN COMBINATORICS AND GRAPH ENTROPY,

J. KÖRNER and K. MARTON, Mathematical Institute of the Hungarian Academy of Sciences, Budapest, P.O.B. 127, H-1364, Hungary.

Record-beating bounds for the problem of perfect hashing have been derived using information theory by Fredman, Komlos and the authors. Perfect hashing is just one example of combinatorial problems that can be interpreted in terms of finding a covering number, i.e., the minimum number of graphs of a predetermined type that cover a given graph. If the graphs K and L have the same vertex set, then their union $K \cup L$ is the graph having the same vertex set and an edge set which is the union of those of K and L. The graph L covers K if $K \cup L = L$.

A covering number in the above sense can be lower bounded by introducing a sub-additive functional on graphs. Korner has suggested using graph entropy, which is a functional $H(G,P)$ defined on graphs G on the vertices of which a probability distribution P is given. For every probability distribution P, $H(G,P)$ is a sub-additive functional, i.e. $H(K \cup L,P) \leq H(K,P) + H(L,P)$. Crucial for combinatorial applications is the tightness of this inequality for various graphs. We are studying conditions under which equality holds when $L = \overline{K}$. A graph K will be called strongly splitting if for every pr.d. on its vertex set $H(P) = H(K,P) + H(\overline{K},P)$. Our main result is that every bipartite graph is strongly splitting. Implications of this and related results will be discussed.

A THEOREM ON DATA COMPRESSION AND ESTIMATION,

BING-ZHENG XU and GUI-QING SHI, South China Institute of Technology, Guangzhou, China.

Usually, the identification process (e.g., in the case of speech identification) consists of two separate processes, one is data compression (rate-distortion coding), and the other is estimation. The identification error thus includes the distortion measure of both the compression and the estimation.

In this paper we give a theorem of data compression and estimation of a single source and its proof.

SESSION MC7

ESTIMATION AND IDENTIFICATION

APPLICATION OF THE LATTICE FILTER TO ROBUST ESTIMATION OF AR AND ARMA MODELS,

SHIPING LI and BRADLEY W. DICKINSON, Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA.

A new method of estimating the parameters of an ARMA model is proposed. A $(p+q)$-stage lattice whitening filter is used to obtain consistent estimates of the AR parameters of an ARMA (p,q) model. It is shown that a set of MA parameter estimates can also be obtained using this approach with little added computation. The method is used for estimation of the AR parameters of an ARMA process in additive white noise. Finally, it is shown that the lattice filter is also useful in robust estimation of the AR parameters of an ARMA process with additive outliers. [This work was supported by NSF Grant ECS84-05460 and by USAF Grant AFOSR-84-0381.]

ASYMPTOTICALLY ROBUST PARAMETER ESTIMATION FOR SIGNALS IN CORRELATED NOISE,

PATRICK A. KELLY, Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003, USA.

Asymptotically robust estimators of location are well-known for cases in which the noise variables are iid or weakly dependent and stationary. The problem of interest here is the extension of those results to the estimation of the amplitude of a known continuous-time signal in correlated, nominally Gaussian noise. The observation is taken to be in $L_2[0,1]$; then by using an orthogonal decomposition the nominal observation may be put in the form of a discrete signal in iid noise. If, however, uncertainty in the noise statistics may result in the noise components in fact having some unknown level of dependence, the previously developed robust estimation methods are not directly applicable. In this paper, we consider some types of uncertainty which allow for dependence and nonstationarity in the noise sequence and for which asymptotically robust estimators can be described. The results follow from noting that the asymptotic distribution of the parameter estimate is not affected by an absolutely continuous change in the measure governing the noise.

THE COVARIANCE-CONSTRAINED MAXIMUM LIKELIHOOD METHOD,

GREGORY H. WAKEFIELD, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109, USA and M. KAVEH, Department of Electrical Engineering, University of Minnesota, Minneapolis, MN 55455, USA.

Certain measurement problems exist for which the general shape of the power spectrum of a random process is more important than resolution of its spectral peaks. Nevertheless, most methods of spectral estimation have been designed and evaluated either implicitly or explicitly, to solve the resolution problem. Given the nonlinear nature of these methods, it isn't clear that high-resolution spectral estimators are appropriate in cases where a high-fidelity estimate, i.e., one that conforms to spectral shape, is desired.

The Covariance-Constrained Maximum Likelihood Method (CCMLM) is a new estimator of the power spectrum which exhibits superior fidelity over that of alternative, high-resolution methods for certain classes of spectra. In this paper, we derive the general form of the CCMLM and discuss an iterative procedure for its implementation. Convergence properties of this procedure are presented and the issue of convergence with respect to a spectral fidelity criterion is raised. Finally, examples of the method's performance for ARMA and non-rational spectra are discussed and compared with those using alternative, high-resolution methods.

THE APPLICATION OF MAXIMUM-ENTROPY AND MAXIMUM-LIKELIHOOD FOR SPECTRAL ESTIMATION,

MICHAEL I. MILLER and DONALD L. SNYDER, Department of Electrical Engineering, Washington University, St. Louis, MO 63130, USA.

We explore the role of the maximum-entropy principle in estimation problems whose data consists of statistical observations from some many-to-one mapping, but where the observations fail to yield moment constraints because there are finitely many data points. Our results are:

1. For likelihood problems resulting from a complete-incomplete data specification, the maximizing density is the conditional density of the complete data, given the incomplete data. The *maxent* density is generated by specifying its domain via the incomplete measurements, rather than as a moment constraint.
2. This identity between the *maxent* density and conditional density indicates that a maximum likelihood problem may be posed as a point entropy maximization, thus providing a basis for iterative solution of a class of likelihood problems.
3. The above is applied to spectral estimation with finite data samples from a stationary Gaussian time series. A complete-incomplete data model leads to maximum likelihood estimates generated by interatively maximizing the entropy function. The convergence point then satisfies conditions for maximizing likelihood in Toeplitz covariance models (see Burg, Luenberger, and Wenger).

RAPID EQUALIZER TRAINING AND CARRIER ACQUISITION IN A VOICEBAND DATA MODEM,

P.R. CHEVILLAT, D. MAIWALD, and G. UNGERBOECK, IBM Zurich Research Laboratory, CH-8803 Ruschlikon, Switzerland.

Fast initial training of a voiceband data-modem receiver employing a transversal equalizer with fractional-T spaced coefficients is considered. A short periodic training sequence without timing preamble is used for gain setting, equalizer training, acquisition of carrier phase and frequency, and symbol synchronization. A joint detection and estimation algorithm is presented for detecting the training signal and estimating carrier-frequency offset. Computation of the equalizer coefficients leads to a constrained optimization problem which is solved efficiently by spectral division. Application of the training method in an experimental high-speed modem which achieves a startup time of 20 msec is discussed.

PLENARY LECTURE*

NONLINEARITIES AND NOISE IN THE REGULATION OF NATURAL POPULATIONS OF PLANTS AND ANIMALS,

ROBERT MAY, Biology Department, Princeton University, Princeton, NJ 08544, USA.

Some natural populations are relatively constant over large periods of time, while others fluctuate greatly from year to year. The simplest mathematical models describing the essential dynamics of such populations are nonlinear. These models can exhibit an astonishing array of dynamical behavior, ranging from stable points, to period-doubling bifurcations that produce a cascade of stable cycles, to apparently random fluctuations; that is, simple deterministic systems can produce chaotic dynamics.

The lecture will show how these ideas illuminate some of the observed properties of real populations in the field and laboratory, and will explore some of the practical implications. When unpredictable environmental fluctuations (in time) and/or heterogeneities (in space) are superimposed on such deterministic models, further complications arise. Some of these complications have to do with disentangling signal from noise in the analysis and interpretation of data: what factors actually regulate the population? Other complications have to do with the practical implications for the management of resources: how should fish quotas be set in an uncertain environment?

*Plenary Lectures will be given in the *Horace H. Rackham Building Lecture Hall*, East Washington Street between State and Fletcher streets.

SHANNON LECTURE*

INVERSION, IDENTIFICATION AND INFORMATION,

WILLIAM L. ROOT, Dept. of Aerospace Engineering and Dept. of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109, USA.

Deterministic signal parameter estimation, determination of an object field using an inverse mapping, and system identification are problem areas with common features as well as differences. After scattered historical remarks, there is discussion of various mathematical models for classes of problems in these areas and the differing points of view involved in choosing these models. For those cases where a considerable amount of information is wanted about an unknown object field or system mapping, for example, the question is raised: under given conditions how much can be determined about the unknown entity? The discussion of this question is tentative.

*Plenary Lectures will be given in The *Horace H. Rackham Building Lecture Hall*, East Washington Street between State and Fletcher streets.

SESSION TA1

PATTERN RECOGNITION I

A PRACTICAL ALGORITHM FOR MINIMAX AND NEAR-BAYES/NEAR-MINIMAX CLASSIFIER DESIGN,

THOMAS E. FLICK, Naval Research Laboratory, Code 6522, Washington, DC 20375, USA and LEE K. JONES, Department of Mathematics, Catholic University of America, Washington, DC 20064, USA.

An iterative technique is developed for finding minimax classifiers. The algorithm uses a gradient search strategy to estimate weights c_i in the nonrandom likelihood-based classifier given by:

$$\text{If } j = arg \max_i c_i p_i(X) \text{ then } X \text{ is assigned to } \omega_j$$

where $p_i(X)$ is the probability density of the random vector X given the class ω_i. A proof is given that the algorithm will converge to the weights of the minimax classifier. Modification of the algorithm to work in an appropriate convex space leads to a near-Bayes/near-minimax classifier, which combines properties of the minimax (low maximum error) with Bayes (low average error). Because of the statistical complexity in most real problems, conditional probabilities of error needed by the algorithm must be estimated. Since it is desired to estimate these rapidly, we develop an approach to rapid error estimation for $p_i(X)$'s as Gaussian mixture distributions. *Examples and numerical results* are included.

EDGE DETECTION USING THE DIRECTIONAL DERIVATIVES OF A CORRELATED RANDOM FIELD MODEL,[†]

YITONG ZHOU, RAMA CHELLAPPA, and V. VENKATESWAR, Signal and Image Processing Institute, PHE-324, University Park, MC-0272, Department of EE-Systems, University of Southern California, Los Angeles, CA 90089-0272, USA.

An edge detector using the first and second directional derivatives of a correlated random field model is described. The method consists of representing the pixels in a window by a $2-D$ causal autoregressive (AR) model, whose parameters are adaptively estimated using a Kalman filter. Due to the modeling assumption, the directional derivatives are functions of AR parameter estimates. An edge is detected if the second derivative in the direction of the estimated gradient is negatively sloped, and the first derivatives and a local estimate of variance satisfy some conditions. Since the causal AR-model-approach results in an oriented edge detector, it may not detect edges whose orientations are significantly different from that of the edge detector. To circumvent this problem, we perform causal AR model based edge detection on the original image and three rotated

[†]Denotes Long Paper

versions of the original image, the rotations being multiples of 90 degrees. The final output is taken as the union of the four edge outputs. The performance of edge detectors is illustrated using synthetic and real images. [Partially supported by the Joint Services Electronics Program, through the Air Force Office of Scientific Research under Contract F 49620-85-C-0071 and by the National Science Foundation under the NSF Grant ECS-84-51010.]

ON A METHOD OF FINDING CONTOUR PROTOTYPES FOR NONPARAMETRIC CLASSIFICATION,

DJORDJE I. JANKOVIĆ, SPIRA M. MATIĆ, and VOJIN E. ZIVOJNOVIĆ,

A number of nonparametric methods of pattern classification suffer from a serious drawback: to classify a new pattern, it is often required that the distance between the new pattern and all patterns in the training set be calculated, and as a consequence, the need to store all training patterns arises. Therefore, a number of procedures for finding prototypes which are to be used in a classifier have been proposed. Contrariwise to the procedures proposed thus far, we propose that every cluster should be analyzed separately. Patterns at the contour of the cluster are selected as prototypes. The decision boundaries are thus optimally preserved. For the 1–*NN* classification rule the error rate for the proposed procedure is the same as if all training patterns were stored. The price we pay for improving the error rate is the greater number of prototypes which is, for present-day computers, still sufficiently small. Another advantage of the proposed procedure is that contour prototypes can be used in a number of other nonparametric classification procedures, which further improves the error rate. The algorithm for finding contour patterns is explained in detail and a comparison with the other mentioned procedures is given.

SESSION TA2

CONSTRUCTION OF TRELLIS CODES

REAL-NUMBER SOURCE-CHANNEL CODING,

TOM G. MARSHALL Department of Electrical Engineering, Rutgers University, Piscataway, NJ 08854, USA.

A structure for combined source-channel coding of real-number sequences is introduced, and a corresponding model employing reflexive generalized inverses for the encoding and decoding matrices is proposed. Block and convolutional implementations employing interpolative coding are discussed. Matrices that are generalized circulant matrices are employed to describe these interpolative structures in the time domain.

Frequency domain descriptions are also used, and they are employed for the convolutional structures as well as for the block structures, thereby extending the frequency domain viewpoint, found useful in block coding to convolutional coding. The convolutional coders make use of multirate structures, familiar in signal processing applications, but new to the field of error correction.

The use of multirate filters as coders is emphasized and illustrated in examples. This approach to coding for error-control suggests that input signal filtering for bandlimiting, regarded here as part of source coding, be simultaneously considered with the filtering required for error control: the proposed model accommodates this viewpoint.

TRELLIS CODING FOR MULTILEVEL PARTIAL RESPONSE PAM AND QAM,

JOHN W. KETCHUM, Telecommunications Research Laboratory, GTE Laboratories, Inc., 40 Sylvan Road, Waltham, MA 02254, USA.

This paper addresses the performance of trellis coded PAM and QAM modulations used in the presence of intersymbol interference, with emphasis on the various forms of partial response signaling. Performance is treated from the perspective of random coding exponents, as well as the performance of optimal or near optimal codes for specific modulation schemes. The performance penalties induced due to the use of partial response are demonstrated and discussed, as is the necessity for precoding with partial response signaling. Some simple trellis codes for use with duobinary $(1 + D)$ and dicode $(1 - D)$ types of partial response channels are presented.

NEW TRELLIS CODES,

A. ROBERT CALDERBANK and N.J.A. SLOANE, AT&T Bell Laboratories, Murray Hill, NJ 07974, USA.

A new technique is proposed for constructing multidimensional trellis codes which provides an alternative to Ungerboeck's method of "set partitioning." The new codes use a signal constellation consisting of points from an n-dimensional lattice Λ, with an equal number of points from each coset of a sublattice Λ'. One part of the input stream drives a generalized convolutional code whose outputs are cosets of Λ', while the other part selects points from these cosets. This technique allows the path multiplicity to be calculated easily. It is also possible to describe methods of differential encoding very simply.

ALGEBRAIC CONSTRUCTION OF LARGE EUCLIDEAN DISTANCE COMBINED CODING/MODULATION SYSTEMS,

R. MICHAEL TANNER, Computer and Information Sciences, University of California, Santa Cruz, CA, USA.

The works of Ungerboeck in designing combined coding and modulation systems by adapting the techniques of convolutional codes and of Ginzburg in designing signal sets by matching algebraic block codes with modulation are extended by exhibiting the construction of power and bandwidth efficient signal sets. Appropriately linking subspaces of an unequal error protection algebraic code with partitioned signals indexed by subspaces of a binary vector space guarantees a large minimum separation between signals in the resulting signal set. For PSK modulations, the "layered" constructions shown have the additional advantage of making the effects of a phase ambiguity "transparent" to the decoding process: the phase ambiguity can be removed after the effects of noise have been eliminated. This resolves phase far more efficiently than does separate phase determining preamble. Using low-complexity soft decision decoding algorithms of Tanner, practical high-speed decoders can be implemented. Simulation studies of one such system show a 6.2 dB gain over 8 PSK at an operating SNR of 12.7 dB with a rate 0.83 code. [Published with the permission of the Ford Aerospace and Communications Corporation, Western Development Laboratory, Palo Alto, CA 94303.]

SESSION TA3

QUEUEING THEORY and QUEUEING NETWORKS

OPTIMAL SCHEDULING POLICIES FOR A CLASS OF QUEUES WITH CUSTOMER DEADLINES TO THE BEGINNING OF SERVICE,

SHIVENDRA S. PANWAR, Department of Electrical Engineering, Polytechnic Institute of New York, Brooklyn, NY 11201, USA, DON TOWSLEY, Department of Computer and Information Science, University of Massachusetts, Amherst, MA 01003, USA, and JACK K. WOLF, Center for Magnetic Recording Research, University of California at San Diego, San Diego, CA, USA.

Many problems can be modeled as single server queues with impatient customers. An example is that of the transmission of voice packets over a packet switched network. If the voice packets do not reach their destination within a certain time interval of their transmission, they are useless to the receiver and considered lost. It is therefore desirable to schedule the customers such that the fraction of customers served within their respective deadlines is maximized. For this measure of performance it is shown that the shortest time to extinction (STE) scheduling policy is optimal for a class of queues. It is also shown, for a wider class of queues, that the optimal scheduling policy belongs to the class of shortest time to extinction with inserted idle times or (STEI) scheduling policies. For one of these queues we compute the expected customer loss using an STE policy and compare its performance with that of the FCFS scheduling policy. [This work was supported by the National Science Foundation, Washington, D.C., under Grant NSF ECS 83-10771.]

SOJOURN TIMES IN JACKSON NETWORKS IN HEAVY TRAFFIC,

V. MADISETTI, S. PAREKH, and J. WALRAND, Department of Electrical Engineering and Computer Sciences and Electronics Research Laboratory, University of California, Berkeley, CA 94720, USA.

We consider the sojourn times of customers in a Jackson network. Results on sojourn time distribution in heavy traffic are rederived, using elementary probabilistic methods. These arguments replace the usual diffusion approximations and provide information on the crucial issue of convergence rates. The distribution of sojourn times is first discussed for the case of simple queues with probabilistic feedback and then extended to the case of a Jackson network in heavy traffic.

Exact results are also derived for a simple example; they illustrate the quality of analytic bounds obtained for the general case.

A POLYNOMIAL COMPLEXITY MEAN VALUE ANALYSIS ALGORITHM FOR MULTIPLE-CHAIN CLOSED QUEUEING NETWORKS,

ADRIAN E. CONWAY, Department of Electrical Engineering, University of Ottawa, Ottawa, Ontario, K1N 6N5, Canada.

A new recursive computational algorithm is presented for the exact analysis of multiple-chain closed networks of queues. It is based on a set of new recursive equations which are in terms of mean performance measures and marginal queue length distributions. The algorithm is a new type of Mean Value Analysis (MVA). The space and time requirements of the algorithm are polynomial in the number of closed routing chains. The requirements are essentially the same as those of the Recursion by Chain Algorithm (RECAL) of Conway and Georganas. The algorithm avoids the computation of normalization constants and represents a solution to the problem of potential numerical overflow or underflow which exists in RECAL. It enjoys the space/time growth characteristics of RECAL as well as the numerical stability which is associated with the well-known MVA algorithm of Reiser and Lavenberg. When there are many routing chains in a network, the proposed algorithm is substantially more efficient than the established MVA algorithm whose complexity is exponential in the number of chains. The algorithm allows one to analyze a wider range of queueing networks by Mean Value Analysis techniques.

SYNCHRONOUS PACKET NETWORKS WITH PRIORITY QUEUEING DISCIPLINES,

AUDREY M. VITERBI, Department of Electrical Engineering, University of California, Irvine, CA 92717, USA.

We study store-and-forward networks involving packetized messages of varying priority classes. The priorities may be established by needs of transmission, as in the case of integrated voice and data networks wherein voice needs to have higher priority for reasonable quality, or by other disparate requirements, where priority is assigned according to other criteria such as length of message or distance from source to destination. Two models are developed to compute the delay experienced by packets of different priorities being multiplexed. The first assumes that the requirements of the various classes are such that each service request is independent of the arrivals of previous service requests of that class. The second Markov model models the dependence of lower priority traffic on that of higher priority traffic by first-order Markov chains. The results are extended to networks with arbitrary topologies.

SESSION TA4

DETECTION THEORY I

A CHARACTERIZATION OF FRACTIONAL BROWNIAN MOTIONS WITH APPLICATIONS TO SIGNAL DETECTION,

R. BARTON and H.V. POOR, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1101 W. Springfield Ave., Urbana, IL 61801, USA.

We consider the problem of detecting a (possibly stochastic) signal $S(t)$ corrupted by a fractional Gaussian noise process $W_H(t)$ having spectral density proportional to f^{1-2H}, $1/2 \leq H < 1$. It can be shown that such a noise process can be regarded as the derivative of a fractional Brownian motion $B_H(t)$ with self-similarity parameter H, which leads us to consider the observation model

$$dY(t) = S(t)dt + dB_H(t) \quad .$$

We exploit a representation of the process $B_H(t)$ which leads naturally to a characterization of the reproducing-kernel Hilbert space (RKHS) of the process as well as an interesting "pre-whitening" result. This allows us to draw some conclusions concerning singularity and equivalence of the detection problem as well as the design of optimum detectors. [This research was supported by the National Science Foundation under Grant ECS-85-12314.]

ON THE NUMBER OF COSTAS ARRAYS AS A FUNCTION OF ARRAY SIZE,

J. SILVERMAN and VIRGIL E. VICKERS, Rome Air Development Center, Electronic Device Technology Branch, Hanscom AFB, MA 01731-5000, USA.

A Costas array or "constellation" is a dot pattern in an $n \times n$ grid with one dot in each row and each column, chosen so that all the $n(n-1)/2$ vectors between dots are distinct. Such patterns, which have minimum-sidelobe aperiodic autocorrelation, are useful for radar and sonar signal design. The values of n for which the number of constellations is known have been extended to $n = 16$. Probabilistic estimation formulae have been developed, based on the assumption of random arrangement of allowed values in the difference triangle, which is ordinarily used to determine whether any particular permutation of the numbers 1 to n corresponds to a constellation. These formulae, which track the exact values from $n = 11$ to $n = 16$ to better than 10%, predict that the number of constellations as a function of n will decrease for $n > 16$, contrary to an earlier conjecture.

ON RESISTANCE IN DETECTION AND PARAMETER ESTIMATION,

KENNETH S. VASTOLA, Electrical, Computer, and Systems Engineering Department, Rensselaer Polytechnic Institute, Troy, NY 12180, USA.

Resistance of detection and estimation procedures using finite memory nonlinearities is considered for arbitrary observation sequences. Resistance (defined originally by Tukey) is a data-dependent version of robustness. (Robustness is concerned with distributions rather than data directly.) A necessary and sufficient condition is given for a procedure to be resistant at all observation sequences.

It is then seen that this "everywhere resistance" is equivalent to everywhere robustness, by which we mean that the procedure is robust at every possible distribution on R^{∞} (the collection of all realizations of discrete-time random processes). Conditions for a strong converse are also discussed and the relationship between resistance and robustness is examined for this case.

These results hold for most practical detection and parameter estimation procedures including time-varying, dependent cases and many common array detection techniques.

OPTIMAL LINEAR-QUADRATIC SYSTEMS FOR DETECTION AND ESTIMATION,

BERNARD PICINBONO and P. DUVAUT, Laboratoire des Signaux et Systèmes, Centre de Recherche du C.N.R.S. et de l'Ecole Superiéure d'Electricité, associé à l'Université de Paris-Sud, L2S-ESE, Plateau du Moulon, 91190 Gif-sur-Yvette, France.

The problem of optimal linear-quadratic systems for detection and estimation without any Gaussian assumption is considered. Usually quadratic systems are used for the detection of stochastic signals in Gaussian noise. Using the deflection criterion, it is shown that the optimal systems for detection can be obtained from a set of coupled linear equations using third and fourth order moments of the noise. Solutions of such equations are given in the case of fourth order white noise and also for spherically invariant processes. It is shown that singular detection can appear with a linear-quadratic structure and disappear with only pure linear or quadratic systems. A relationship between detection and estimation is proved in the case of linear-quadratic systems, extending some results known only in the linear case. [This work was partially supported by the Direction Technique des Constructions Navales, contract N85.48.826.072 from Groupe d'Etude et de Detection sous-marine du Brusc.]

SESSION TA5

BLOCK CODE PERFORMANCE

A NOTE ON THE COMPUTATION OF BIT ERROR RATE FOR BINARY BLOCK CODES,

MICHELE ELIA, Dipartimento di Elettronica, Politecnico di Torino, Corso Duca degli Abruzzi 24, I-10129 Torino, Italy.

Bit error probability versus the error probability of the binary symmetric channel is derived for linear block codes having a transitive group of symmetry. A linear homogeneous differential transformation of the weight enumerator allows us to obtain a closed expression for the bit error probability assuming standard array decoding with coset leaders appropriately chosen: that is, coset leaders are taken as either the unique element of minimum weight, if any, or, as the unique element with all zeros in the information positions.

MORE ON THE DECODER ERROR PROBABILITY FOR REED-SOLOMON CODES,

KAR-MING CHEUNG and ROBERT J. McELIECE, Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125, USA.

This paper is an extension of a recent paper by McEliece and Swanson dealing with the decoder error probability for Reed-Solomon codes (more generally, linear MDS codes). McEliece and Swanson offered an upper bound on $P_E(u)$, the decoder error probability given u symbol errors, which is only slightly larger than Q, the probability that a completely random error pattern will cause decoder error. In this paper we derive an exact formula for $P_E(u)$, which is useful for numerical calculations, and a set of lower bounds on $P_E(u)$, which yield insight into the problem. For example we can show that for all u, $P_E(u)$ is lower bounded by $C(\frac{q-2}{q-1})^t P_E(d-t)$, where C is a "correction factor" which is close to 1.

We use our exact formula to calculate the $P_E(u)$'s for the (255,223) RS (NASA) code, and the (31,15) RS (JTIDS) code. These numbers show that $|\frac{P_E(u)}{Q} - 1|$ tends to zero rapidly as u gets large, and our lower bound on $P_E(u)$, combined with McEliece and Swanson's upper bound, allow us to give an analytic proof of this result.

A NOTE ON PERFORMANCE OF NEW TYPE 4-STEP DECODER FOR PRODUCT CODE,

CHU-ICHI SODEYAMA and HARUO KONDO, Technological University of Nagaoka, Department of Electrical Engineering, Nagaoka, Niigata, 949-54 Japan.

In this paper we propose a new type 4-step decoder for product codes having high decoding speed and high code reliability, and investigate the performance of the decoder for product codes.

The probability of a decoding bit error at each step of several versious of the 4-step decoder is calculated, and the most profitable decoding algorithm is found.

It is shown that the way of using information flags at every step of multi-step decoder has important influence upon the probability of a decoding bit error and that the probability of decoding bit error can be reduced when the information flags are used at only the final step.

The relationship between the decoding delay time and the calculating time of the syndrome components is traced. It is shown that the calculating time of syndrome components occupy a major part of the decoding delay time, and the syndrome components of the every step can be more simply calculated from the syndrome components of the preceding step. This reduces the decoding delay time.

The probability of the decoding bit error of the proposed decoder at the symbol error rate $=10^{-2}$ is reduced to less than 10^{-13}, and the decoding delay time is finally reduced to less than 0.75 that of the ordinary 4-step decoder.

ERROR DETECTING CAPABILITIES OF THE SHORTENED HAMMING CODES ADOPTED FOR ERROR DETECTION IN IEEE STANDARD 802.3,

TORU FUJIWARA and TADAO KASAMI, Faculty of Engineering Science, Osaka University, Toyonaka, Osaka, 560 Japan, and SHU LIN, Department of Electrical Engineering, Texas A&M University, College Station, TX 77843, USA.

In this paper, we investigate the error detecting capabilities of the shortened Hamming codes adopted for error detection in IEEE standard 802.3. These codes are also used for error detection in the data link layer of the Ethernet, a local area network. The generator polynomial of these codes is a primitive polynomial of degree 32. Let C_n denote the shortened code of length n. In the Ethernet the code length n is a multiple of 8 greater than 511 and less than 12145. We compute the weight distribution of the dual code of C_n for various code lengths. Using MacWilliams' identity we show that the minimum distance of C_n is 5 for $512 \leq n \leq 3006$, and 4 for $3007 \leq n \leq 12144$. For $n = 2^p$ with $9 \leq p \leq 13$ and $n = 12144$, we compute the probability of undetectable error and that of detectable error for a binary symmetric channel with bit-error-rate $10^{-5} \leq \epsilon \leq 1/2$. For nonnegative integers b less than 17, we compute the maximum code length n_b such that C_{nb} has the capability of detecting any double-burst-error pattern which consists of two burst errors of length b or less.

SESSION TA6

SHANNON THEORY II

CAPACITY OF PEAK AND AVERAGE POWER CONSTRAINED QUADRATURE GAUSSIAN CHANNELS,

SHLOMO SHITZ, ISRAEL BAR-DAVID, and RUBEN MICHEL, Department of Electrical Engineering, Technion - Israel Institute of Technology, Haifa 32000, Israel.

The time-discrete (TD) quadrature additive Gaussian channel (QAGC) is a model for time-continuous signalling schemes, e.g. quadrature amplitude modulation (QAM), for which the input signal and the output observations can be represented by sample points in a two-dimensional space. We investigate the capacity $C(\rho_p,\rho_a)$ of a TDQAGC under peak-and average-power limitations, ρ_p and ρ_a, respectively, and show that the distribution of the input signal that achieves capacity is discrete in amplitude and uniform in phase, by using properties of Schwartz spaces and optimization theorems. Furthermore, we derive rather tight bounds on $C(\rho_p,\rho_a)$ as well as the limiting probability distributions of the signal for small and for large ρ_p and ρ_a. In the case of peak-power limitation only, for normalized $\rho_p \leq 7.8db$, the optimum input is a phase-modulated constant-amplitude signal. At larger values of ρ_p several amplitude levels (including 0) become necessary. At very large ρ_p the amplitude distribution becomes linear. This work is an extension of Smith's derivations of capacity in one-dimensional input space. The results may serve as a yardstick to those of Einarsson and Saleh and Salz who considered the cut-off rate under similar constraints.

CODING BOUNDS FOR HIGH SIGNAL-TO-NOISE RATIO GAUSSIAN NOISE CHANNELS,

ROBERT G. GALLAGER, Laboratory for Information and Decision Systems. Massachusetts Institute of Technology, Cambridge, MA 02139, USA.

The random coding bound, using a shell constraint, for a memoryless discrete time additive Gaussian noise channel in the limit of large signal to noise ratio is given by $P_e \leq \exp - NE_r(R)$, where P_e is expected error probability, N is constraint length, R is the rate in nats, and $E_r(R)$ is the reliability function. We show that

$$E_r(R) = \begin{cases} [\exp(2C - 2R) - 1]/2 - (C - R) & ; \quad 0 < C - R < \\ R_{comp} - R & ; \quad C - R < \end{cases}$$

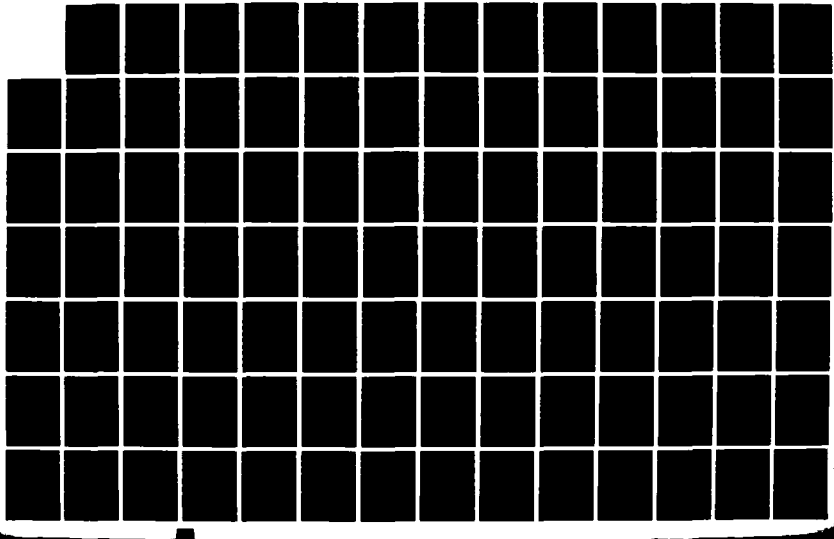
where

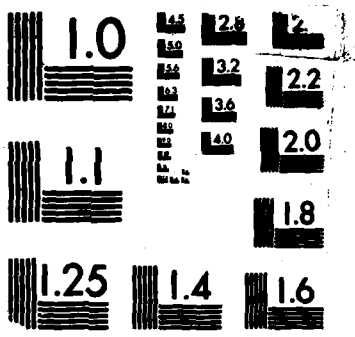
$$R_{comp} = C \quad \ln 2 \cdot 1 \quad 2$$

Note that R_{comp} is 1.68 dB below
ing without a shell constraint
distribution of signal
sional sphere

AD-A193 252 IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY (ISIT): ABSTRACTS OF P..(U) MICHIGAN UNIV ANN ARBOR ROBINSON OCT 86 AFOSR-TR-88-0287 AFOSR-87-0046 2/3

UNCLASSIFIED F/G 12/9 NL





MICROCOPY RESOLUTION TEST CHART
BUREAU OF STANDARDS-1963-A

such a channel is interpreted in light of these results, which help to explain why set partitioning can operate so close to channel capacity.

ACHIEVABLE RATES FOR A CONSTRAINED GAUSSIAN CHANNEL,†

L. OZAROW and A.D. WYNER, AT&T Bell Laboratories, Murray Hill, NJ 07974, USA
and J. ZIV, Technion Institute of Technology, Technion City, Haifa, Israel.

We consider a continuous-time channel where the input waveform $x(t)$ is constrained to take on but two values, i.e., $x(t) = \pm\sqrt{P}$, where P is the signal power. The signal is passed through a linear filter and added to white Gaussian noise. With a suitable choice of filter, this channel is a model of the channel corresponding to a magnetic storage medium.

We are interested in the channel capacity, C_O, of this channel, and in particular the relation of C_O to C_P and C_{AV}, where C_P is the capacity of the same channel with the two-level constraint on $x(t)$ replaced by the "peak-power" constraint $|x(t)| \leq \sqrt{P}$, and C_{AV_T} the capacity of the channel with the (classical) "average-power" constraint $\frac{1}{T}\int_0^T x^2(t)dt \leq P$, for large T. It has been known for some time how to compute C_{AV}.

Of course $C_O \leq C_P \leq C_{AV}$, and one of our main results is the surprising fact that $C_O = C_P$. We cannot find $C_O = C_P$ exactly, but in this paper we obtain, for certain filters, lower bounds which are fairly close to C_{AV}.

---

†Denotes Long Paper

SESSION TB1

PATTERN RECOGNITION II

ON MULTI-LEVEL THRESHOLD FUNCTIONS,

SVERRIR 'OLAFSSON and YASER ABU-MOSTAFA, California Institute of Technology, Pasadena, CA USA.

The threshold element, extensively studied by Cover [*IEEE Trans. Elect. Comput.*, Vol. EC-14, pp.326-334, 1965], Minsky [*Perceptrons*, MIT PRess, 1969] and Muroga (among others), can be extended in a natural way to a multi-level threshold element. The input weighting mechanism remains the same, and without significant increase in cost one adds a somewhat more complex thresholding scheme. In this paper we show this gives a roughly N^k-fold increase in the number of separable dichotomies, where N is the number of input points and k is the number of thresholds. One may hence conclude that the role of multiple thresholds is of similar importance as the number of dimensions in the input space.

THE CONSISTENCY PROBLEM OF STATISTICAL INDEPENDENCE ASSUMPTIONS,

RANGASAMI L. KASHYAP and YIZONG CHENG, School of Electrical Engineering, Purdue University, West Lafayette, IN 47907, USA.

Many probabilistic reasoning systems employ formulae for combining evidence based on Bayes' theorem and one or more statistical independence assumptions for evidence. Suppose there are n mutually exclusive hypotheses and m pieces of evidence. The formulae for combining evidence are to calculate the posterior probability $P(h_i)$ and the individual impact $P(h_i \mid e_j)$, $j = 1, \ldots, m$, for each hypothesis h_i, where e_j are evidence. By invoking different statistical independence assumptions, the formulas for combining evidence are totally different and provide different results. Three independence assumptions have been used in the literature of expert systems and pattern recognition. These assumptions are: conditional independence on atomic hypotheses (*CIA*, $P(e_1, \ldots, e_m \mid h_i) = P(e_1 \mid h_i) \cdots P(e_m \mid h_i)$ for each i); conditional independence on the negation of atomic hypotheses (*CIN*, $P(e_1, \ldots, e_m \mid \neg h_i) = P(e_1 \mid \neg h_i) \cdots P(e_m \mid \neg h_i)$ for each i); and global independence (*GI*, $P(e_1, \ldots, e_m) = P(e_1) \cdots P(e_m)$).

We show that under simultaneous assumptions of *CIA* and *CIN* ($n > 2$, otherwise they are the same assumption), among the m evidences $e_1, \ldots, e_m$, at least $\max[0, m - \lfloor n/2 \rfloor]$ evidences are completely irrelevant, that is, $P(h_i \mid e_j) = P(h_i)$ for all i and at least $\max[0, m - \lfloor n/2 \rfloor]$ j's. For example, when $n = 3$ and $m = 2$, one of the two evidences must be completely irrelevant. On the other hand, simultaneous assumptions of *CIA* and *GI* creates difficulties in the reconciliation of the assignment of prior probabilities and individual impact because an awkward relation exists among these values.

This study justifies that the most adequate formula for combining evidence in a probabilistic reasoning system is $P(h_i \mid e_1, \ldots, e_m) = KP(h_i)\ \Pi_{j=1}^{m}[P(h_i \mid e_j)/P(h_i)]$ where K is a normalization factor. This is the formula based on the assumption of conditional independence of evidence on each atomic hypothesis (*CIA*).

ON DECISION TREES FOR PATTERN RECOGNITION,

PHILIP A. CHOU and ROBERT M. GRAY, Information Systems Laboratory, Dept. of Electrical Engineering, Stanford University, Stanford, CA 94305, USA.

The pattern recognition problem is formulated as a communications problem so that rate-distortion bounds can be applied. In particular, decision trees are viewed as variable-length encoder/decoder pairs. For small problems, the optimal performance of decision trees is obtained by exhaustive enumeration, and compared to the theoretical limits given by the rate-distortion function. Although simulations show that decision tree performance improves with blocklength, analytic results for certain sources show that the performance of decision trees is bounded away from the rate-distortion function. Practical decision trees designed by greedy algorithms are found to compare favorably with optimal trees under certain conditions. [This work was supported by the National Science Foundation (Grant No.IST 85 09860).]

APPLICATION OF RATE-DISTORTION THEORY TO PATTERN CLASSIFICATION AND CONTROL SYSTEM REGULATION,

SALVATORE D. MORGERA, Department of Electrical Engineering, McGill University, McConnell Engineering Building - Rm. 514, 3480 rue Université, Montréal H3A 2A7 Québec, Canada.

Shannon's rate-distortion theory is applied to problems in pattern recognition and classification and control system regulation. Both applications can be viewed as communications channels and generalizations of data compression or source coding. We assume, however, as have Wolf and Ziv, that the "source output" may be distorted prior to encoding and, furthermore, the "decoder output" may be distorted prior to its delivery to the final destination. This interpretation permits the formalization of interesting trade-offs between classifier complexity and error rate on one hand, and controller complexity and residual error on the other. Several examples are provided for different source statistical dependence and structural models. [This work supported by Canada NSERC GRant A0912.]

SESSION TB2

ALGEBRAIC CODING

SOME NOTES ON THE BINARY WEIGHT DISTRIBUTION OF REED-SOLOMON CODES,

KYOKI IMAMURA, W. YOSHIDA, and N. NAKAMURA, Saga University, Saga, 840, Japan.

Recently Kasmi and Lin (1984 and ISIT '85) presented the binary weight distributions of some Reed-Solomon codes and their extended codes. In this paper, first, the explicit formula for the binary weight distributions are presented and shown to be independent of the choice of the basis for $GF(2^m)$ in case of two $(n = 2^m - 1, k = 2)$ Reed-Solomon codes over $GF(2^m)$ generated by the polynomials $(x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{n-2})$ and $(x - 1)(x - \alpha) \cdots (x - \alpha^{n-3})$, where α is a primitive element of $GF(2^m)$. These Reed-Solomon codes belong to the set of the dual codes discussed by Kasami and Lin and our formulas are much simpler: It is shown that the weight of each codeword of the binary $(nm,2m)$ linear code obtained from the $(n,2)$ Reed-Solomon code generated by $(x - 1)(x - \alpha) \cdots (x - \alpha^{n-3})$ takes one of the following three values: $0, (m - 1)2^{m-1}$, and $m2^{m-1}$. Second, it is proved that the binary weight distribution of an $(n = 2^m - 1, k)$ Reed-Solomon code $(1 \leq k \leq n - 1)$ with respect to the basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is the same as that with respect to the bases $\{\beta_1^2, \beta_2^2, \ldots, \beta_m^2\}$. Third, simple numerical examples are given to show that the binary weight distribution of a Reed-Solomon code generally depends on the choice of the basis.

CYCLIC CODES WEIGHT ENUMERATION IN THE TRANSFORM DOMAIN,

JEAN CONAN and FRANCIS LANGLOIS, Departement de Génie Electrique, Ecole Polytechnique de Montréal, PO Box 6079 Station "A", Montréal, Québec, H3C 3A7 Canada.

Given $(n,q) = 1$ and m the multiplicative order of q modulo n, cyclic codes over $GF(q)$ with length n can be mapped into n-tuples over $GF(q^m)$ through a Galois-Fourier transformation making use of a primitive nth root of unity of $GF(q^m)$. It is shown that the cyclic characteristic of the codes is reflected by the cancellation of specific spectral components corresponding to indices which belong to a union of q-chains of Z_n. For minimal cyclic codes only one q-chain is implicated from which it becomes easy to identify elementary cycle representatives in the spectral domain. The Hamming weight of these specific codewords can be easily computed without Fourier inversion through the use of either Euclid's algorithm or any minimal partial realization procedure for rational sequences such as the Wilkinson-Morf-Kailath algorithm. The results are furthermore applicable to non-minimal codes by using a spectral version of an extension of a result due to van Lint and which is implementable on a computer. Taking into account the efficiency of computer based Fourier transformers, it is believed that this approach should be able to deal with larger block and information lengths than previously possible with the more classical direct methods.

SOME NEW CONSTRUCTIONS FOR BINARY CONSTANT WEIGHT CODES,

IIRO HONKALA, Department of Mathematics, University of Turku, SF-20500 Turku 50, Finland.

We give some lower bounds for $A(n,d,w)$, the maximum cardinality of a binary constant weight code of length n, minimum distance d and constant weight w. When the minimum distance is ten or greater very many good constructions are not known. We give some simple methods which give some improvements to the best known lower bounds. We build a new constant weight code starting from a code and a binary constant weight code of shorter lengths. In this way we e.g. prove that $A(27,12,9) = 39$. If there is a conference matrix of order $n = 4k$ and of order $n + 2$ or $n/2$ we show that $A(2n+1,n,n-1) \geq 3n$, which shows that $A(17,8,7) \geq 24$ and $A(25,12,11) \geq 36$. In the same way we can also prove other bounds, e.g., $A(21,10,9) \geq 25$ and $A(22,10,9) \geq 30$.

BOUNDS ON THE MINIMUM DISTANCE OF CYCLIC CODES VIA BOUNDS ON THE LINEAR COMPLEXITY OF PERIODIC SEQUENCES WITH KNOWN PATTERNS OF ZEROS,

THOMAS SCHAUB, Central Research and Development, Landis & Gyr, CH-6301 Zug, Switzerland and JAMES L. MASSEY, Institute for Signal and Information Processing, Swiss Federal Institute of Technology, CH-8092 Zurich, Switzerland.

The linear complexity of a sequence of digits is defined as the length of the shortest linear feedback shift-register (LFSR) that can generate the sequence when loaded with its initial digits. A theorem, implicit in the work of Blahut, connects the length N discrete Fourier transform (DFT) to linear complexity. Blahut's theorem asserts that the Hamming weight of the length N time-domain sequence equals the linear complexity of the (semi-infinite) periodic frequency-domain sequence.

For a cyclic (N,K) code over $GF(q)$ whose length N is relatively prime to the characteristic of the field, the $N - K$ roots of the generator polynomial specify the locations of the $N - K$ zeros within one period of length N of the DFT sequence. The minimum linear complexity of a non-zero periodic sequence with these zero locations is thus a lower bound on the Hamming weight of every non-zero codeword and hence on the minimum distance of the code. Bounds on the minimum complexity of periodic sequences with specific zero-location patterns are derived and used to bound the minimum distance of cyclic codes. The BCH bound, the Hartmann-Tzeng bound and the Van Lint-Wilson bound are all shown to be subsumed under this linear complexity approach.

SESSIONS TB3

NETWORKS: PROTOCOLS AND FLOW CONTROL

CHARACTERIZATION OF INFORMATION FLOW IN AN URBAN PACKET RADIO NETWORK,

WILLIAM S. HORTOS, Lockheed Electronics Company, Systems Analysis Group, 7500 Commerce Center Drive, Orlando, FL 32819, USA.

The dynamics of information flows within a packet radio network operating in an urban environment are determined not merely by the bursty exogenous inputs at the terminals, but also by the signalling conditions on the radio links between nodes that form the changing network configuration. This makes the operation of radio networks very different from cable-based computer-communications networks. The factors that establish link availability in a dense, urban environment are multipath fading and delay, man-made interference, and Doppler fading for ground-based radio nodes, both mobile and fixed.

Based on theoretical and empirical models of these factors, a set of matrix-valued, stochastic functions is defined for the node-to-node link availability. At a given time the value of the (i,j) entry of the matrix represents the fractional availability of the link between radio i and radio j in the network.

ROUND ROBIN SCHEDULING FOR FAIR FLOW CONTROL IN DATA COMMUNICATION NETWORKS,

ELLEN L. HAHNE and ROBERT G. GALLAGER, Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.

A simple strategy is proposed for achieving fair session throughputs in a point-to-point packet network with virtual circuit routing. Each link offers its packet transmission slots to its user sessions in round robin fashion. In addition, conventional window flow control is used to prevent excessive queues at bottleneck links. Under certain simplifying assumptions it can be proved that, as the window size increases, the session throughput rates approach limits that are perfectly fair in the max-min sense. (By this we mean that the smallest session rate in the network is as large as possible and, subject to that constraint, the second-smallest session rate is as large as possible, etc.) For the case where all sessions have heavy demand, a finite window size suffices to produce perfectly fair session throughputs, but for some networks the required window size is impractically large. If small windows are used, it is possible to achieve approximate fairness of session throughputs, as well as reasonable packet delay.

CENTRALIZED AND DECENTRALIZED OPTIMAL FLOW CONTROL PROTOCOLS IN COMPUTER COMMUNICATION NETWORKS,

AUREL A. LAZAR, Dept. of Electrical Engineering and Center for Telecommunications Research, Columbia University, New York, NY 10027, USA.

A unified treatment for modeling and optimal control in computer communications networks is presented. The criterion employed maximizes the average throughput under an average time delay constraint. It is demonstrated that for queueing networks modeling computer communication networks a separation theorem between flow control and estimation holds. The problem of optimal routing and flow control is reduced to a problem of optimal routing. Linear and dynamic programming methods as well as majorization arguments are used to derive the structure of the optimal control policies.

PERFORMANCE OF AN INTEGRATED POLLING/RESERVATION SCHEME FOR METROPOLITAN AREA NETWORKS,

IZHAK RUBIN and ZSEHONG TSAI, Electrical Engineering Dept., 6731 Boelter Hall, University of California, Los Angeles, CA 90024, USA.

We consider a metropolitan area communication network, consisting of many bursty data terminals, distributed over a wide geographical range. Applications include packet-radio networks, whereby terminals share a single multi-access frequency-band through time-division access schemes, and inter-connections of local area networks over a wide-area geographical region. In both cases, a single access control algorithm, such as polling (or token), random-access or reservation scheme, can prove to be inefficient, due to the wide geographical distribution of stations, leading to long propagation delay and acquisition-time factors. To alleviate these problems, we present and study here a hybrid access-control procedure.

An integrated Polling/Reservation scheme is presented for metropolitan area multi-access communication networks containing large populations of terminals. The channel access right circulates among groups of terminals according to a polling discipline. Once a primary group-terminal is polled, secondary local terminals belonging to the polled group can access the channel according to a reservation scheme. Without specifying the specific reservation procedure, a general analytical technique for carrying out message delay analysis is presented.

An explicit expression for the mean message delay for symmetric systems is obtained. The result is also useful for obtaining upper and lower bounds for the mean message delay.

SESSION TB4

CODES IN EUCLIDEAN SPACE

ON THE CONSTRUCTION OF THE BEST SPHERICAL CODE BY COMPUTING THE FIXED POINT,[+]

DEJAN E. LAZIĆ, T. BECE, and P.J. KRSTAJIĆ, Faculty of Technical Sciences, Institute for Measurement and Control, 21000 Novi Sad, V.Vlahovića 3, Yugoslavia.

In this paper a continuous mapping of the a set of all spherical codes into itself is found. It is demonstrated that one of the fixed points of this mapping has to be the best spherical code, or a code as close to it, in terms of minimal distance, as needed. An iterative algorithm is evaluated that always converges to one of the fixed points of the mapping considered. A table of the minimal distances of the spherical codes obtained in this way is given, for various dimensions (up to 12) and sizes (up to 128). From the table it can be seen that the difference between minimal distances of various codes of the same dimension and size obtained in this way is always negligible.

A NEW UPPER BOUND ON THE DENSITY OF SPHERE PACKINGS IN THREE DIMENSIONS,

DOUGLAS J. MUDER, The MITRE Corporation, Burlington Road, Bedford, MA 01730, USA.

It is widely believed that in a close packing of identical spheres in R^3, the smallest Voronoi polyhedron is the regular dodecahedron. If this could be proved, the best upper bound on the density of such a packing would be reduced to .7547 $\cdots$. Using a notion of local density due to Rogers, this paper proves that the optimal face of a Voronoi polyhedron is a regular pentagon slightly smaller than the pentagonal faces of the dodecahedron. This establishes an upper bound of .77836 $\cdots$ on the density, a marginal improvement on the best previous upper bound, recently proved by Lindsay. It is also shown that the best 3-sided and 4-sided faces are regular triangles and squares, respectively.

[+]Denotes Long Paper

ON THE STRUCTURE OF GROUP CODES FOR THE GAUSSIAN CHANNEL,

INGEMAR INGEMARSSON, Institutionen for Systemteknik, Department of Electrical Engineering, Linkoping University, S-581 83 Linkoping, Sweden.

A group code for the Gaussian channel is a set of vectors in the Euclidean N-space for which the maximum-likelihood decision regions are congruent. The group code is invariant under multiplication with a group G of orthogonal matrices. The code may be generated from G by multiplication with an initial vector. We have shown that the subgroup H which leaves the initial vector invariant can not be self-conjugate if it is a proper subgroup of G.

The set $\{O_i\}$ in G transforms any one of the code vectors to all the code vectors. We have shown that $\{O_i H\}$ are cosets to H in G and that the set $\{O_i\}$ transforms any one of the cosets to all the cosets.

We have also introduced the concept of subcodes. A subcode is invariant under multiplication with a subgroup of G. A subcode divides the original codes into clouds around every vector in the subcode. We have derived conditions under which the clouds are congruent.

SESSION TB5

INVESTMENT AND GAMBLING THEORY

UNIVERSAL ALGORITHMS FOR GAMBLING, DATA COMPRESSION, AND PORTFOLIO SELECTION,

PAUL H. ALGOET, Boston University College of Engineering, 110 Cummington Street, Boston, MA 02215, USA.

Let $\{X_t\}_{-\infty<t<\infty}$ be a stationary ergodic process with an unknown distribution, and let $\overline{P}_\infty$ denote a regular conditional probability distribution of the next outcome X_0 given the infinite past X_{-1}, X_{-2}, etc. We review and extend a procedure due to Ornstein and Bailey, to learn $\overline{P}_\infty$ from past experience. The procedure generates estimates $\widetilde{P}_1, \widetilde{P}_2, \ldots, \widetilde{P}_k, \cdots$ such that $\widetilde{P}_k \Rightarrow \overline{P}_\infty$ weakly almost surely. The estimate $\widetilde{P}_k$ will be a function of past observations $X_{-1}, \ldots, X_{-p_k}$ where $p_k = p_k(\omega)$ is a stopping time and $p_k \to \infty$ more or less fast, depending on the particular realization ω and the degree of confidence desired for $\widetilde{P}_k$.

Let $\hat{P}_t$ denote the last output of the procedure when it is fed the sequence $X_{t-1}, \ldots, X_0$ but not yet X_{-1}. Then P_t is a computable approximation of $\overline{P}_\infty \circ T^t$, the true but unknown conditional distribution of X_T given the infinite past. The performance of decisions based on the surrogate $\hat{P}_t$ matches that of optimum decisions based on the true conditional distribution $\overline{P}_\infty \circ T^t$, in the long run when averages are taken over many periods. This leads to universal algorithms for gambling, data compression, and portfolio selection.

UNIFORMLY GOOD PORTFOLIOS,

THOMAS M. COVER, Stanford University, Stanford, CA 94305, USA.

We investigate a new sequential portfolio selection algorithm in which no assumptions are made about the sequence of stock market values. The resulting capital S_n at time n can be proved to outperform the Value Line (the m^{th} root of the product of the m stocks in the market) for all n and for all market sequences. (This opens up obvious trading opportunities, since it is possible to trade Value Line in the market.) Moreover, S_n outperforms the best stock S_n^* to first order in the exponent, i.e., $\underline{\lim}\frac{1}{n}\ln\frac{S_n}{S_n^*} \geq 0$, for all stock sequences. In particular, if the stock vectors are independently identically distributed, then $S_n = e^{nW^*+0(\sqrt{n})} \to \infty$, where W^* is the highest possible exponent. The proofs are based on analysis of a portfolio sensitivity matrix that can be shown to play the same role in portfolio theory that the Fisher information matrix plays in estimation theory.

The portfolio algorithm in this paper represents a different point of view from the algorithm of Cover and Gluss ("Empirical Bayes Stock Market Portfolios," *Advances in*

Applied Mathematics, 1986), which was based on Blackwells' approach-exclusion theory. In addition to dominating Value Line, it achieves the same objectives as the algorithm of Cover and Gluss, with slightly improved second order terms and removal of discreteness conditions.

ROBUST INVESTMENT,

DAVID C. LARSON, IBM Almaden Research Center, San Jose, CA 95120, USA.

Let stock prices be represented by a discrete, positive sequence of vectors, where the proportionate change in price of a given stock during a given investment period is chosen from a finite set of possible values. No distribution on stock prices is assumed. We exhibit a sequential portfolio strategy that ϵ-achieves the rate of growth of capital attained by the log-optimal portfolio based on prior knowledge of the n-period empirical distribution. Moreover, for a horse race model, we exhibit a betting strategy which earns money at an exponential rate and earns within a polynomial factor as much money as the log-optimal portfolio based on prior knowledge of the n-period empirical distribution of winners and *end-play*. This result holds for every sample sequence. It corresponds to universal noiseless coding. It suggests that a similar result holds for the more general stock market model. In addition, these investment strategies are much easier to compute than the Cover-Gluss strategy. [This research was partially supported by the National Science Foundation under Grant ECS82-11568.]

MAXIMUM ENTROPY AND THE LOTTERY,

HAL STERN AND THOMAS M. COVER, Stanford University, Stanford, CA, USA.

In the typical lottery game, each player's ticket consists of a set of m distinct integers chosen from among the first M integers. All entrants whose m number match the winning set of numbers share the first prize. Applying Csiszár's conditional limit theorem, the probability distribution of a ticket conditioned on the observed proportion of tickets containing each integer is the maximum entropy probability mass function subject to the same constraints. Iterative proportional fitting is proposed as an algorithm for computing this distribution. This distribution is used to determine which numbers to select on a ticket in order to beat the parimutuel payoff.

SESSION TB6

SHANNON THEORY III

SHANNON STRATEGIES APPLIED TO THE DEFECT CHANNEL,

J.P.M. SCHALKWIJK, Department of Electrical Engineering, Eindhoven University of Technology, Den Dolech 2, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

Using Shannon's results on channels with side information at the transmitter, we will show that if the channel defects are known to the sender it is possible to replace the defect channel by an equivalent noisy channel with feedback. Feedback strategies for these noisy channels can now be translated into optimal codes for the original channel with defects. We will give several examples. For the binary defect channel we can thus reliably transmit information at rates up to the channel capacity $C = 1 - p$, where p is the expected fraction of defects.

INFORMATION CAPACITY OF THE GAUSSIAN CHANNEL WITH FEEDBACK,

CHARLES R. BAKER, Department of Statistics, University of North Carolina, Chapel Hill, NC 27514, USA.

It has long been conjectured that the information capacity of the Gaussian channel can be increased by adding feedback. However, only fragmentary results are known, and no general proof has been published. In fact, it is well-known that the capacity cannot be increased if the channel is "matched": that is, the constraint on the message process is given in terms of the covariance of the channel noise.

In this paper, it is shown that the capacity of the finite-dimensional mismatched Gaussian channel is always increased by feedback if the noise is correlated. In particular, when the transmitted signal is subject to a pure power constraint, then the capacity is always increased by feedback when the channel noise is correlated. Expressions are also given for the capacity. Additional results are given for the infinite-dimensional mismatched channel.

THE CAPACITY OF PERMUTING RELAY CHANNELS,

KINGO KOBAYASHI, Department of Biophysical Engineering, Faculty of Engineering Science, Osaka University, Toyonaka, Osaka 560 Japan.

Blackwell's trap door channel is a famous example of a finite state channel. Its deterministic versions, that is, permuting channels, have been studied by Ahlswede and Kaspi in a multi-terminal information theoretic framework. They determined the capacity of permuting jammer and relay channels for some special cases. In this paper, we completely solve the problem for permuting relay channels. More precisely, when α is the cardinality of the alphabet, and β is the number of available storage locations in the channel, the capacity $C_R(\alpha,\beta)$ of the permuting relay channel is given by $\log \lambda$, where λ denotes the maximum eigenvalue of a matrix Q derived from the channel state transition mechanism.

FEEDBACK INCREASES CAPACITY OF GAUSSIAN CHANNELS BY AT MOST HALF A BIT,

SANDEEP POMBRA and THOMAS M. COVER, Stanford University, Stanford, CA, USA.

Let C denote channel capacity and C_{FB} channel capacity for the same channel with the addition of feedback. Shannon has shown $C_{FB} = C$ for memoryless channels. However, feedback increases capacity for channels with memory. Pinsker and Ebert have shown $C_{FB} \leq 2C$ for arbitrary nonwhite additive Gaussian noise channels. (We give a new proof here.) We then prove that $C_{FB} \leq C + \frac{1}{2}$ (bits/unit time). The proofs are based on the inequalities

$$|K_{X+Z}|^{\frac{1}{2}} |K_{X-Z}|^{\frac{1}{2}} \leq |K_X + K_Z|$$

and

$$|K_{X+Z}| \leq |2K_X + 2K_Z| \quad .$$

SESSION TC1

CONSTRUCTION OF CONVOLUTION AND TRELLIS CODES

RATE COMPATIBLE PUNCTURED CONVOLUTIONAL CODES AND THEIR APPLICATION TO FADING CHANNELS AND UNEQUAL ERROR PROTECTION,

J. HAGENAUER, German Aerospace Research Establishment (DFVLR), D-8031 Oberpfaffenhofen, West Germany.

The concept of punctured convolutional codes is extended to find rate compatible punctured convolutional (RCPC)-codes, where punctured code bits of a low rate code are simultaneously used as punctured bits for the higher rate code. Such code families have been found for memories up to 6 and rates between 1/3 and 8/9. Their distance spectrum is given and allows analytical performance calculations on several types of channels. Applications of Viterbi-decoding of RCPC-codes are the inner code with varying rate of a modified type II ARQ system with interleaving on a fading channel using channel state information and soft decoding of time varying unequal error correcting codes.

FAST ALGORITHMIC CONSTRUCTION OF MOSTLY OPTIMAL TRELLIS CODES,

JAN-ERIK PORATH and TOR AULIN, Chalmers University of Technology, Division of Information Theory, S-412 96 Göteborg, Sweden.

The area of trellis channel coding has gained recent interest, especially the schemes with integrated coding and modulation. Whatever the specific scheme is, there is a great need to find the best possible one within a given structure. A dynamic programming approach is proposed here for a fast construction of good convolutional codes (in the sense of maximizing the minimum free Euclidean distance $d^2_{\min}$ which is a common criteria of goodness). Present methods use exhaustive search among all codes together with symmetry properties among the codes. This approach gets impractical very soon.

Earlier work in this area was done by S. Lin, H. Lyne and D.J. Costello. It should be remembered that the well known Viterbi algorithm was not available at that time.

The trellis schemes that we consider have shift registers as memory units and from the contents of these, channel symbols are chosen by the use of a given function. Each transition in the trellis is labeled with some channel symbol, one for each transition. It is this labeling that we want to optimize with respect to $d^2_{\min}$.

Our algorithm is tested on several schemes with coding rates $R = (n-1)/n$. The results is compared with the best codes known in each case and very often they will be optimal or as good as the best known codes for a given scheme. [This work was supported by the National Swedish Board for Technical Development under Grant 84-3317.]

ON THE USE OF THE LEE-METRIC IN CONSTRUCTING CONVOLUTIONAL CODES,

JAAKKO T. ASTOLA, Lappeenranta University of Technology, Lappeenranta, Finland.

It is well known that the Lee-metric provides a rather realistic distance function in the construction of codes for a phase modulated channel. In this paper the Lee-distance properties of convolutional codes are studied. It is easy to see that the free Lee-distance of a q-ary convolutional code is bounded by

$$\begin{cases} \frac{q+1}{4} L & \text{if } q \text{ is even} \\ \frac{q^2}{4(q-1)} L & \text{if } q \text{ is odd} \end{cases},$$

where L is the constraint length. It is shown that this bound can only be achieved by memory one codes. Moreover a class of such codes is constructed. The results of a computer search for good rate $1/2$ memory one and two codes is presented.

A NEW METHOD OF CONSTRUCTING CONVOLUTIONAL CODES ON THE BASIS OF SUPERIMPOSED CODES,

TOHRU INOUE, Information and Electronics Development, Mitsubishi Electric Corp., Kamakura, 247, Japan, and MASAO KASAHARA and TOSHIHIKO NAMEKAWA, Faculty of Engineering, Osaka University, Suita 565, Japan.

We propose two new methods of constructing convolutional codes on a basis of product codes.

Method 1 uses the superimposing codes with smaller minimum distances compared with those of conventional methods.

We have also proposed another method (Method 2) which can eliminate some portion of check symbols of the ground codes without destroying the error-correcting capability.

Method 2 also yields a new coding scheme which achieves different reliability on a specific part of a codeword.

In this paper, we discuss on these methods and obtain a new conventional codes which can be considered as a combined version of CSOCs and Wyner-Ash codes. The newly constructed parameters of the codes is tabulated.

ANALYTIC DESIGN OF CONVOLUTIONAL ENCODERS,

PETER F. SWASZEK, Department of Electrical Engineering, University of Rhode Island, Kingston, RI 02881, USA.

Binary convolutional encoders are classified by their constraint length L, the number of input bits k, and the number of output bits n with the coder's details contained in an $L \times n$ binary interconnection matrix $\mathbf{H}$ (with rows $\mathbf{h}_i$). Performance is typically measured through free distance. Previously published results on maximum free distance are for particular triplets $\{L,k,n\}$ and rely upon computer searches over the class of all interconnection matrices.

This paper presents an analytic approach to the maximization of free distance which a priori fixes only L and k. The technique first computes the free distance as a function of the L unknown rows of $\mathbf{H}$ and then selects the $\mathbf{h}_i$ to maximize this function. It involves specifying the encoder's state diagram (with branch weights being functions of the $\mathbf{h}_i$) and computing the encoder's transfer function through Mason's gain formula, keeping only those terms relevant to the free distance.

As an example let $L = 3$ and $k = 1$. It is shown that both $\mathbf{h}_1$ and $\mathbf{h}_3$ should be n-vectors of all ones and $\mathbf{h}_2$ should be an n-vector containing $\lfloor 2n/3 \rfloor$ ones ($\lfloor x \rfloor$ means greatest integer $< x$). With this selection the free distance is $\lfloor 8n/3 \rfloor$ which exactly matches Heller's upper bound on free distance. Details of the technique and further examples are presented in the paper.

NOTES

SESSION TC2

OPTICAL COMMUNICATIONS II

COHERENT OPTICAL COMMUNICATION SYSTEMS,‡

VINCENT W.S. CHEN, Massachusetts Institute of Technology, Lincoln Laboratory, Lexington, MA 02173, USA.

Over the past few years, coherent optical communication systems using semiconductor lasers have become an area of considerable research and development at many research laboratories. Application scenarios include fiber and space communication systems. Based on preliminary experimental results, there is no doubt that coherent communication with semiconductor lasers is possible at least in a qualitative way. However, semiconductor lasers are very far away from being perfect lasers, exhibiting complicated frequency and intensity noise processes. What remains to be demonstrated in that system design can exploit fully the advantages but finesse the many imperfections of semiconductor lasers. In this paper we will review recent results and present open problems on system design and analysis peculiar to coherent semiconductor laser communication systems. This will include modulation/demodulation and coding issues, time and frequency acquisition and tracking. In particular, we will contrast this unconventional "nonclassical" channel with the conventional additive white Gaussian channel and indicate how proper system designs may yield performances very close to those resulting from systems using ideal lasers as components. [This work was sponsored by the Department of the Air Force. The views expressed are those of the author and do not reflect the official policy or position of the U.S. Government.]

SQUEEZED STATE PHOTODETECTION,‡

JEFFREY H. SHAPIRO, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.

This talk surveys the general semiclassical and quantum treatments of photodetection. Most of this material is tutorial, however, some fundamental points of contention remain, and results for closed-loop configuration are just becoming available.

The output quantities of interest for an ideal photodetector are the photocurrent $i(t)$ and the photocount record $N(t)$, where the latter is related to the former by integration, and both are classical stochastic processes. Under rather general conditions, both the semiclassical and quantum treatments imply that $N(t)$ is a self-exciting counting process, whose statistics can be expressed in terms of multicoincidence rates (MCRs).

The semiclassical and quantum theories characterize the MCRs in terms of classical and quantum electromagnetic fields, respectively. In conventional open-loop operation, these statistics have been worked out in detail. Here is is known that the semiclassical approach gives quantitatively correct answers when the quantum field is classical, i.e., the field is in a Glauber coherent state or a classically random mixture of such states. Also, there are unmistakable signatures for non-classical states that are detected open-loop,

‡Denotes Invited Paper

such as sub-Poisson photocounts or sub-shot noise photocurrent spectra. It is the nonclassical behavior of squeezed-state light that leads to its dramatic signal-to-noise ratio gain over coherent state light in homodyne detection.

In closed-loop configurations, it turns out that there are no clear signatures for nonclassical state behavior. Indeed, the open-loop quantum photodetection statistics of an arbitrary light beam state can be obtained from closed-loop semiclassical theory by appropriate choice of the feedback function. Through use of a quantum non-demolition measurement, this may lead to a synthesis procedure for arbitrary quantum states. [This research was supported in part by NSF Grant ECS 84-15580.]

CUT-OFF RATE FOR QUANTUM COMMUNICATION CHANNEL WITH INDEPENDENT COHERENT STATES,

M. CHARBIT and C. BENDJABALLAH, Laboratoire des Signaux et Systèmes du C.N.R.S., Ecole Supérieure d'Electricité, Plateau du Moulon, 91190 - Gif sur Yvette, France.

Use of the cut off rate criterion for evaluating the performance of a direct detection optical channel is analyzed from the quantum point of view. An M-ary communication channel is considered and the formula of R_0 as given by Massey is assumed to be valid for the quantum case provided that we substitute $Tr[\rho_i P_j]$ for the transition probability distribution. The ρ_i is the density operator of the state $i(i=1, \ldots, M)$ and the $P_j(j=1, \ldots, M)$ is taken as a projector valued measure (p.v.m.) characterizing the output. First we study the case of M linearly independent pure states and establish a new upper bound on R_0 given by $R_0 \leq \sum_k \sum_l \ln g'_{kl}$ where g'_{kl} is the element of the inverse of the matrix of the scalar products $g_{kl} = (\phi_k \mid \phi_l)$. We then seek the conditions for which this bound is reached. Analytical results are obtained for g_{kl} positive. A particular case of practical interest, namely coherent states with $g_{kl} = \exp\left[-\frac{s}{2}(k-1)^2\right]$, is treated in detail for some values of M. Finally comparison with the Gaussian quasi-classical channel shows that the quantum optimum is of superior performance as expected. [Supported by E.N.S.T. (UA 820 du C.N.R.S.), 46 rue Barrault, 75013 - Paris (France).]

SESSION TC3

RANDOM PROCESSES II

UNIFORMIZATION FOR SEMI-MARKOV DECISION PROCESSES UNDER STATIONARY POLICIES,*

FREDERICK J. BEUTLER, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109, USA and KEITH W. ROSS, Department of Systems Engineering, University of Pennsylvania, Philadelphia, PA, USA.

Uniformization permits the replacement of a semi-Markov decision process (SMDP) by a Markc chain exhibiting the same average rewards for simple (non-randomized) policies. It is shown that various anomalies may occur, especially for stationary (randomized) policies; uniformization introduces virtual jumps with concomitant action changes not present in the original process. Since these lead to discrepancies in the average rewards for stationary processes, uniformization can be accepted as valid only for simple policies.

We generalize uniformization to yield consistent results for stationary policies also. These results are applied to constrained optimization of SMDP, in which stationary (randomized) policies appear naturally. The structure of optimal constrained SMDP policies can then be elucidated by studying the corresponding controlled Markov chains. Moreover, constrained SMDP optimal policy computations can be more easily implemented in discrete time, the generalized uniformization being employed to relate discrete and continuous time optimal constrained policies.

VON MISES COLLECTIONS AND UNSTABLE RANDOM SEQUENCES,

ADRIANOS PAPAMARCOU and TERRENCE L. FINE, School of Electrical Engineering, Cornell University, Ithaca, NY 14853, USA.

We are interested in modelling nondeterministic time series in which it appears that the random variables are uniformly bounded, there are no discernible nonstationarities, and time averages do not converge. As is well known, there is no stationary probability measure assigning positive probability to such a collection of sample sequences.

The approach of R. von Mises to fequentist probability relies upon place selection rules to causally generate subsequences of a given sample sequence. If the subsequences of infinite length, generated by a large enough collection of place selection rules, share the frequentist properties (limits of averages) of the original sequence, then the sequence is called a collective, and it is considered to be a random sequence. We have examined the possibilities for the use of families of place selection rules to characterize randomness among those sample sequences whose time averages are divergent. We provide conditions under which such sample sequences exist.

---

*Denotes Long Paper

A STUDY OF RELATIONSHIPS BETWEEN MARKOV-TYPE RANDOM PROCESS MODELS,

WENLONG ZHANG, HALUK DERIN, and PATRICK A. KELLY, Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003, USA.

Widespread use of Markov processes in one and two dimensional signal modeling has resulted in many different related Markov-type process characterizations, whose relationships have not always been explicitly and clearly stated. This is particularly true of two dimensional field models commonly used in image processing. This paper presents a careful study of the relationships, equivalences and implications among different Markov-type processes. The classes of Markov processes considered are strict-sense Markov (SSM) vs. wide-sense Markov (WSM); causal vs. non-causal; Gaussian vs. non-Gaussian; and under causal class Markov mesh, quarter plane and non-symmetric half-plane models; and under non-causal class Markov random field, Gibbs random field, Markov-P, weakly Markov, strongly Markov, conditional Markov and simultaneous autoregressive models. This systematic charting of the Markov Scene will include many well-known relationships as well as some new ones that have not been noted previously. A representative few of these relationships are: the equivalence of causal and non-causal classes for SSM processes in 1-D, equivalence of Markov-P and MRF models, and necessary and sufficient conditions for non-causal AR process driven by a regular process to be WSM. [This work was supported by NSF Grant NSF-ECS-8403685 and ONR Grant N00014-85-K-0561.]

INNOVATIONS AND WOLD DECOMPOSITIONS OF STABLE SEQUENCES,

STAMATIS CAMBANIS, Center for Stochastic Processes, Department of Statistics, University of North Carolina, Chapel Hill, NC 27514, USA, CLYDE D. HARDIN, Jr., The Analytic Sciences Corporation, One Jacob Way, Reading, MA 01867, USA, and ALEKSANDER WERON, The Institute of Mathematics, Technical University, 50-370 Wroclaw, Poland.

For symmetric stable sequences, notions of innovation and Wold decomposition (WD) are introduced, characterized, and their ramifications in prediction theory are discussed. As the usual covariance orthogonality is inapplicable, the non-symmetric James orthogonality is used, thus leading to right and left innovations and Wold decompositions, which are related to regression prediction and least p^{th} moment prediction, respectively. Independent innovations and WD are also characterized; and several example illustrating the various decompositions are presented. [This work was supported by AFOSR Contract F49620 82 C 0009.]

SESSION TC4

CONTINUOUS PHASE MODULATION

A DECOMPOSITION APPROACH TO CPM,

BIXIO RIMOLDI, The Institute for Communication Technology, ETH-Zentrum, 8092 Zurich, Switzerland.

An interesting modulation scheme for nonlinear and/or fading channels having both spectral economy and good power performance is Continuous Phase Modulation (CPM). In this paper we show that CPM systems can always be decomposed into a Continuous-Phase Encoder (CPE) and a Memoryless Modulator (MM) in such a way that the CPE is a linear (modulo some integer p) time-invariant sequential circuit and the MM is also time-invariant. Such a decomposition has two advantages. First, it permits the "encoding" operation to be studied independently of the modulation. This might suggest alternative realizations of the encoder (and hence alternative implementations of CPM) and also suggests alternative forms of the optimum decoding algorithm. Moreover, because the CPE is time-invariant and linear, it can be studied by the same techniques that have been developed for convolutional encoders which are also time-invariant linear (over a finite field) systems. Moreover, if the CPE were linear over a finite field $GF(p)$ the CPE itself would be a convolutional encoder, and the cascade of an outside convolutional encoder with the CPE would reduce to an equivalent single convolutional encoder. The second advantage of such a decomposition of CPM is that the isolation of the MM allows one to model the cascade of the MM, the waveform channel [that we assume is characterized by Additive White Gaussian Noise (AWGN)], and the demodulator that operates over one symbol interval, as a Discrete Memoryless Channel (DMC). The cut-off rate and capacity of this DMC can then be studied without the distractions introduced by the CPE.

M-ARY MULTI-T PHASE CODERS,

PAWEF SZULAKIEWICZ and WITOLD HOFUBOWICZ, Technical University of Poznan, Institute of Electronics and Communications, ul. Piotrowo 3 A, 60-965 Poznan, Poland.

This paper considers the minimum Euclidean distance properties, upper bounds on the minimum distance, synchronisation properties and power-bandwidth tradeoffs for M-ary phase codes where K different symbol lengths are used in a cyclical manner. When these lengths are all related to each other as rational numbers, they give a finite state Markov chain (trellis) description of the signal. In this paper $K = 2$ is assumed.

It is found that from the point of view of minimum distance and spectral properties multi-T phase codes are very similar to multi-h codes. It is also shown that quaternary codes give considerable improvement over binary codes. An example of a synchronisation

circuit is described. In the phase tree for multi-T codes there are increasing and decreasing straight lines (this is not true for the multi-h codes) corresponding to discrete frequencies above or below the carrier frequency. This implies that multi-T codes are easier to synchronize than multi-h codes.

CODED CPM - A PARAMETER TRADEOFF AND COMPARISON TO CODED QAM,

GORAN LINDELL Telecommunication Theory, University of Lund, Box 118, S-221 00 Lund, Sweden, and CARL-ERIK SUNDBERG, AT&T Bell Laboratories, Crawford Hill Laboratory, HOH L163, Holmdel, NJ 07733, USA.

Continuous phase modulation (CPM) is a class of digital modulations with constant amplitude. By combining CPM with convolutional coding and by maintaining the phase continuous at all times, schemes which are jointly power and bandwidth efficient can be constructed. It is assumed that the channel is the additive white Gaussian noise channel and that the ideal coherent receiver performs maximum likelihood sequence estimation. In this paper we report on bit error probability vs bandwidth tradeoff for a wide range of code rates and CPFSK schemes. The coding is applied to a variable number of bits per CPM symbol and also to one or several successive CPM symbols. The results are based on bounds on the coded systems thus identifying parameter regions where good coded systems can be found. We also compare constructive coded CPM schemes to trellis coded QAM systems in terms of bit error probability and bandwidth.

DISTANCE PROPERTIES OF TRELLIS CODED CPFSK SIGNALS,

N. EKANAYAKE and R. LIYANAPATHIRANA, Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, Newfoundland, A1B 3X5, Canada.

This paper considers the distance properties of uncoded M-ary continuous phase frequency shift keyed (CPFSK) signals and trellis coded CPFSK signals, when the receiver consists of a phase detector followed by a trellis decoder. Previous investigations have been limited to correlation demodulation followed by trellis decoding. Our results for uncoded CPFSK signals show that phase detection and trellis decoding yield superior distance properties than correlation type detection for modulation indices $\leq 1/M$. Motivated by these results, the investigation is extended to trellis coded CPFSK signals. The minimum distance results for trellis coded CPFSK signals also indicate that phase detection yields larger minimum distance than correlation detection for small values of the modulation index. We also make the observation that trellis decoding of coded CPFSK signals is transparent to the unresolved carrier phase ambiguities. Since the phase detector is much easier to implement than the correlation detector, the new results presented should make CPFSK signaling a more attractive alternative to PSK signaling.

MINIMUM DISTANCE AND BANDWIDTH OF MULTI-AMPLITUDE CPFSK SIGNALS,

MICHAEL G. MULLIGAN, Department of Electrical and Computer Engineering, Northeastern University, 360 Huntington Avenue, Boston, MA 02115, USA, and JOHN W. KETCHUM, Telecommunications Research Laboratory, GTE Laboratories, Inc., 40 Sylvan Road, Waltham, MA 02254, USA.

The search for power and bandwidth efficient modulation techniques has produced on the one hand continuous phase modulation schemes such as Minimum Shift Keying (MSK), and on the other hand large rectangular signal constellations known collectively as Quadrature Amplitude Modulation (QAM). There is a bridge between these two areas in the work of several authors who have shown a connection between a variation of MSK, namely Multi-Amplitude MSK (MAMSK), and an offset-keyed version of QAM.

In this paper we consider a generalization of MAMSK based upon the realization that MSK is a very specific case of Continuous Phase Frequency Shift Keying (CPFSK). Thus we present here a modulation technique which we will refer to as Multi-Amplitude CPFSK, and of which MAMSK is a specific case. A general description of the modulation is presented first, in both mathematical and graphical form. This is followed by a discussion of the distance properties of the signals. An upper bound on the minimum distance is presented and the situations in which this bound is achieved are explained. Finally we present a closed-form expression for the bandwidth of these signals along with plots of the power density spectrum and out-of-band power.

NOTES

SESSION TC5

FILTERING

DISCRIMINATION INFORMATION AS THE FIDELITY MEASURE FOR MODELING AND FILTERING PROCESSES,

FERNANDO LEPE, ANDRÉS BUZO, and FEDERICO KUHLMANN, Universidad Nacional Autónoma de México, Facultad de Ingeniería, División Estudios de Posgrado, P.O. Box 70-256, 04510, D.F., Mexico.

Minimizing the mean squared error (MSE) has traditionally been the most common criterion used in a great variety of signal processing applications. Among the advantages of this method, we can mention the fact that for linear processing, only second-order statistics of the involved processes are required for designing optimal systems. Besides, if the processes are Gaussian, then designs based on second order statistics are optimal. On the other hand, methods based on the maximum entropy principle, and discrimination information (or cross-entropy), have successfully been used to derive new results, or to give new interpretations to results based on MSE, in signal processing applications. In this paper we present simple derivations of some of the relevant properties of discrimination information between processes, as well as some interpretations which allow applying this as the design criterion for optimally filtering, predicting and modelling of processes. These results complement those obtained by minimizing MSE, and can be applied to classical problems like the Wiener filter design.

STATISTICAL THRESHOLD DECOMPOSITION FOR RECURSIVE AND NON-RECURSIVE MEDIAN FILTER,

GONZALO R. ARCE, Department of Electrical Engineering, University of Delaware, Newark, DE 19716, USA.

The statistical analysis of recursive non-linear filters is generally difficult. The analysis of recursive median filters has been limited to the trivial cases of signals with a small number of quantization levels and to small window sizes. In this paper we develop a block-state description of recursively filtered signals and apply this description to threshold decomposition to obtain closed-form expressions for the statistics of recursive median filters. In this case, the number of quantization levels and window size do not increase the analysis complexity since the output statistics depend on the distribution of a single, thresholded and filtered binary signal. The statistical decomposition is also developed for non-recursive median filter operations yielding a connection from classical order statistics to the threshold decomposition approach. Finally, some statistical properties are derived for recursively median filtered signals. [The author gratefully acknowledges the support of the National Science Foundation under the grant No. ECS 830-7764.]

A FAST ALGORITHM FOR LINEAR ESTIMATION OF THREE-DIMENSIONAL HOMOGENEOUS ANISOTROPIC RANDOM FIELDS,

ANDREW E. YAGLE, Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109, USA.

This paper presents a fast algorithm for estimating a three-dimensional homogeneous random field from noisy observations inside a sphere of finite radius. It thus constitutes an alternative to solving a multi-dimensional Wiener-Hopf equation. The algorithm is fast in that it exploits the structure of the integral equation kernel to reduce the computation required to construct the optimal filter. It is thus an extension of similar fast algorithms that have been obtained for the one-dimensional and isotropic random field estimation problems. The algorithm works in two stages. First, the optimal filter for the causal problem of estimating the random field at the edge of the sphere of observations is recursively computed as the radius of the sphere is increased. Next, the optimal filter for the non-causal smoothing problem of estimating the random field in the interior of the sphere is computed from the causal filter. For the special case of estimating anisotropic random field at the center of a sphere of observations, the algorithm is shown to reduce to an algorithm derived previously for this problem.

ANALYTIC AND NUMERICAL RESULTS IN RANDOM FIELDS ESTIMATION THEORY,

A.G. RAMM, Mathematics Department, Kansas State University, Manhattan, KS 66506, USA.

Let $u(x) = s(x) + n(x)$, $x \ o \ R^r$, be a random field observed in a domain $D \subset R^r$. Let $Lu = \int_D h(x,y)udy$ be a linear estimate of As, where A is a given operator. The problem is to find the estimate optimal in the following sense $\overline{(Lu - As)^2} = \min$. Here the bar denotes mean value, $s(x)$ is a useful signal, $n(x)$ is noise, $\bar{s} = \bar{n} = 0$, and the covariance functions $\overline{u^*(x)u(y)} = R(x,y)$ and $\overline{u^*(x)s(y)} = f(x,y)$ are known. No assumptions about distributions of random fields are made. The optimal estimate is defined by the function $h(x,y)$. This function is a solution to the multidimensional integral equation (1) $\int_D R(x,z)h(z,y)dz = f(x,y), x,y \in D \cup \partial D$, if $A = I$, i.e., if we deal with the filtering problem. A theory of equation (1) is given. Numerical methods for solving (1) are suggested.

OUTLIER RESISTANT FILTERING AND SMOOTHING,

HARALAMPOS TSAKNAKIS and P. PAPANTONI-KAZAKOS, EECS Department, U-157, University of Connecticut, Storrs, CT 06268, USA.

We consider a stationary Gaussian information process transmitted through an additive noise channel. We assume that the noise and information processes are mutually independent, and we model the noise process as nominally Gaussian with additive independent outliers. For the above system model, we first develop a theory for outlier resistant filtering and smoothing operations. We then design specific nonlinear operations, and we study their performance. The performance criteria are the asymptotic mean squared error at the Gaussian nominal model, the breakdown point, and the influence function. We find that our operations combine excellent nominal model performance with strong resistance to outliers. [This work was supported by AFOSR grant AFOSR-83-0229.]

NOTES

SESSION TC6

SHANNON THEORY IV

BOUNDS ON THE ENTROPY SERIES,

RENATO CAPOCELLI, A. De SANTIS, and I.J. TANEJA, Dipartimento di Informatica ed Applicazioni, Universita di Salerno, 84100 Salerno, Italy.

Upper bounds are furnished for the entropy of a countable random variable, that takes integer values, in terms of the expectation of the logarithm function.

In particular, an upper bound is derived that is sharper than the upper bound of Elias $H(P) \leq E_P(\log) + 2(1 + \sqrt{E_P(\log)})$ whatever is $E_P(\log)$. Bounds that are better only for large values of $E_P(\log)$ than the previous known upper bounds are also provided.

ESSENTIAL AVERAGE MUTUAL INFORMATION,

ERIC MAJANI, OLIVER COLLINS and YASER ABU-MOSTAFA, California Institute of Technology, Pasadena, CA, USA

The problem of essential average mutual information has been by Cover and Copinath. $I_K(X;Y)$ is the largest possible mutual information of the form $I(X;\hat{Y})$, where $\hat{Y}$ is a compression of Y assuming at most K values. Every $I(X;\hat{Y})$ corresponds to a partition of the N outputs into K sets.

The following notations will be used: $J = \{1, 2, \ldots, N\}$ is the set of output indices; for $j \in J$, Y_j is the j^{th} output, $r_j = Pr(Y=Y_j)$ and $I(X;Y) = \Sigma_{j\in J} r_j I(X;Y_j)$; for $k \in \{1, 2, \ldots, K\}$, $\hat{Y}_k$ is the k^{th} output of $\hat{Y}$, and $I(X;\hat{Y}) = \Sigma_{k=1}^{K} Pr(\hat{Y}_k) \cdot I(X;\hat{Y}(k))$. Our main result is:

$$\frac{K-1}{N} < R(M,N,K) \leq \frac{K-1}{N-1} \quad .$$

THE INFORMATION ENTROPY OF THE CHINESE LANGUAGE,

VICTOR K. WEI, Bell Communications Research, 435 South Street, Morristown, NJ 07960, USA.

The entropy of a language is the average amount of information produced by each letter of a typical text. It is the minimum average number of bits needed to represent each letter in the typical text, using the most efficient method of encoding. In his pioneering work on the subject, C. Shannon devised an experiment and determined that the entropy of printed English is less than 1.3 bits. Recently, T. Cover devised another experiment which uses a gambling game to estimate the entropy of English.

In this paper, we apply Cover's experiment to the Chinese language to obtain a gambling estimate of its entropy. The result is that the entropy of the Chinese language is less than 4.1 bits per character.

and their translations. We show that the translation process often gains in information content.

ON WEAK ASYMPTOTIC ISOMORPHY OF MEMORYLESS CORRELATED SOURCES,

K. MARTON, Mathematical Institute of the Hungarian Academy of Sciences, Budapest, P.O.B. 127, H-1364, Hungary.

Let $\{(X_i, Z_i)\}$ be an i.i.d. sequence of random pairs in a finite set $\mathbf{X} \times \mathbf{Z}$; we will call it a discrete memoryless stationary correlated (DMSC) source with generic distribution dist(X_1, Z_1). Two DMSC sources $\{(X_i, Z_i)\}$ and $\{(X'_i, Z'_i)\}$ are called asymptotically isomorphic in the weak sense if for every $\epsilon > 0$ and sufficiently large n, there exists a joint distribution dist(X^n, Z^n, X'^n, Z'^n) of n-length blocks of the two sources such that

$$\frac{1}{n} H(X^n \mid X'^n) < \epsilon, \quad \frac{1}{n} H(Z^n \mid Z'^n) < \epsilon,$$

$$\frac{1}{n} H(X'^n \mid X^n) < \epsilon, \quad \frac{1}{n} H(Z'^n \mid Z^n) < \epsilon.$$

For single sources of equal entropy, McMillan's theorem implies asymptotic isomorphy in the sense suggested by this definition. For correlated sources, however, no nontrivial cases of weak asymptotic isomorphy are known, and, adopting a somewhat more restrictive definition, it turns out that DMSC sources cannot be isomorphic in a non-trivial way.

The main results of this talk are:

(i) Some spectral properties of the generic distribution are invariant for weak asymptotic isomorphy;

(ii) For a large class of DMSC sources, if a source in this class is asymptotically weakly isomorphic to another DMSC source (not necessarily in this class) then the generic distributions of the two DMSC sources are isomorphic.

NOTES

PLENARY LECTURE*

SPREAD SPECTRUM MULTIPLE ACCESS: THE PRACTICE AND THE PROMISE,

ANDREW J. VITERBI, Qualcomm, Inc. and University of California, San Diego, CA, USA.

Spread spectrum techniques have been employed for a variety of useful purposes including interference rejection, accurate ranging, multipath rejection and for coexisting on a channel without interfering or without being detected.

Spread spectrum for multiple access (SSMA) by a large number of partly unregulated users is a technique which is receiving much attention for such potential applications as mobile telephony (with either satellite or terrestrial repeaters), and data transfer among many low-cost, low-power terminals. These developments have aroused considerable controversy between practitioners favoring and opposing this use of the RF spectrum.

We shall address the pros and cons of spread spectrum multiple access, review previous system applications and theory and introduce some new considerations. In particular, relatively unregulated SSMA will be compared with tightly controlled non-interfering demand-assigned time-or-frequency-division multiple access (DAMA), in the context of large distributed networks employing terminals with low individual duty factors.

Passing from practice to promise, some new results will be presented showing that SSMA can overcome its reputation for spectural inefficiency and, through a process of "successive cancellation," achieve higher efficiencies than more conventional non-interfering multiple access techniques, particularly when all transmitters are limited to generating only constant envelope signals.

---

*Plenary Lectures will be given in The *Horace H. Rackham Building Lecture Hall*, East Washington Street between State and Fletcher streets.

SESSION WA1

CONSTRUCTION OF MODULATION CODES

BLOCK CODES FOR THE 2^n-PSK CHANNEL,

HENK C.A. VAN TILBORG, Departement of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, The Netherlands and LI FUNG CHANG, Bell Communications Research, Morristown, NJ 07960, USA.

In 1977 Imai and Hirakawa describe how n binary block codes can be combined to construct block codes for the 2^n-PSK channel. Using this technique it is quite easy to construct block codes for this channel with very high asymptotic coding gains.

This result only seems to have theoretical value, because good soft decision decoding algorithms seldom exist for these codes. For the 8-PSK channel we show how three nearly trivial, binary linear codes together form a block code, that has a very simple maximum-likelihood decoding algorithm. Its performance and complexity is comparable with Ungerboeck's $v = 2$ convolutional code.

MATCHED ENCODERS IN COMBINED CONVOLUTIONAL ENCODING AND MEMORY-SYSTEMS,[*]

F. MORALES-MORENO and S. PASUPATHY, Department of Electrical Engineering, University of Toronto, Toronto M5S 1A4, Canada.

An approach to optimize the combination of an (n,k) convolutional encoder $\mathbf{G}$ and a known memory-system S is introduced. The objective is to maximize the free Euclidean-distance (FED) for a given rate-k/n and given number of states in the combined code-trellis, i.e., for a given Viterbi decoder complexity (VDC). Minimum-shift keying (MSK) and $(1\pm D)$ partial response channels are studied in detail. It is shown that for a given VDC the best combinations are obtained by using a matched encoder $\mathbf{G} = \mathbf{G}_{ma}$, where $\mathbf{G}_{ma}$ is an encoder whose code-trellis has X states, where X is the maximum value such that $X \leq Y$, and Y is the number of states in the combined code-trellis. The conventional approach optimizes the coded memory-system for a given constraint-length of $\mathbf{G}$, and not for a given VDC. Mismatched encoders are identified with the conventional approach, and it is shown that, for same VDC comparisons, matched encoders $\mathbf{G}_{ma}$ are in general superior over mismatched encoders $\mathbf{G}$. Particular results show that when S has feedback, some catastrophic $\mathbf{G}_{ma}$ produce signal-space codes free of catastrophic error propagation. Conditions for the above are established. By introducing differential encoding/decoding techniques it is shown that the best combinations of $\mathbf{G}$ and S can be obtained from matched encoders generating codes with maximum free Hamming distance.

---

[*]Denotes Long Paper

CONSTRUCTION, ANALYSIS AND DECODING OF CODES AND LATTICES VIA PARTITIONS AND TRELLISES,[†]

G. DAVID FORNEY, Motorola, Inc., 20 Cabot Blvd., Mansfield, MA 02048, USA.

Most trellis-coded modulation schemes can be shown to be based upon partitions of certain integer lattices of dimension $N = 2^n$, namely the "main sequence" (Barnes-Wall) lattices and their "principal sublattices." These lattices are themselves useful as dense packings of N-space for moderate N. This paper gives a simple construction (the "squaring construction") which generates all these lattices, determines their dimensionality as binary vector spaces, their minimum distances, and their duality and other properties; it also shows the interrelationships of these lattices to each other and to Reed-Muller codes. An extension of this construction yields lattices and related codes of length $N = 3 \times 2^n$, including the Leech lattice and Golay code. The lattices and codes generated by these constructions may be regarded as "coset codes," namely as sequences of cosets of lower-dimensional lattices or codes that are selected by a binary encoder. They may be represented by trellis diagrams that not only display their structure and interrelationships but also lead to efficient maximum likelihood decoding algorithms.

[†]Denotes Long Paper

SESSION WA2

CRYPTOGRAPHY

A PUBLIC-KEY CRYPTOSYSTEM BASED ON THE DIFFICULTY OF SOLVING A SYSTEM OF NON-LINEAR EQUATIONS,

SHIGEO TSUJII, Dept. of Electrical and Electronic Engineering, Faculty of Engineering, Tokyo Institute of Technology, 2-12-1 O-okayama, Meguro-ku, Tokyo, 152 Japan, KAORU KUROSAWA, Dept. of Information Processing, Graduate School at Nagatsuta, Tokyo Institute of Technology, 4259 Nagatsuta, Midori-ku, Yokohama, 227 Japan, TOSHIYA ITOH and ATSUSHI FUJIOKA, Dept. of Electrical and Electronic Engineering, Faculty of Engineering, Tokyo Institute of Technology, and TSUTOMU MATSUMOTO, Division of Electrical and Computer Engineering, Faculty of Engineering, Yokohama National University, 156, Tokiwadai, Hodogaya-ku, Yokohama, 240 Japan.

Only a few public-key cryptosystems have been proposed, and these possess disadvantages such as the need for intensive computation. For example, RSA requires $O(m^3)$ operations, where m is the message block size. We proposed a public key cryptosystem, which is based on a set of nonlinear equations, and which requires less computation but more memory that RSA. The proposed system has the following properties:

1. The computational complexity of encryption and decryption are $O(m^2)$.
2. A digital signature is possible.

Two methods of attack against the cryptosystem are considered. It is shown that both require an excessively large number of computations when the key bit size $k \geq 6$.

The system is suitable for hardware realization because encryptation and decryptation are performed in $GF(2^t)$. Since the public key is constructed by simple arithmetic operations, fast transformation is achieved by parallel or pipeline processing.

A PRACTICAL AND FAIR PROTOCOL FOR SIGNING CONTRACTS,

K. TAKARAGI, T. SHIRAISHI, and R. SASAKI, Systems Development Laboratory of Hitachi Ltd., Kawasaki, Japan.

Suppose that two persons, A and B, are going to sign a contract over a communication network with a security center which can function only in troubled situations. Our major concern is how to safely exchange the digital signatures under the limited computer and transmission loads in both the normal exchange and the arbitration of troubles. Digital signatures, first introduced by Diffie and Hellman, can be proof of contract agreement after they have been exchanged. In our protocol, three ciphers, i.e., B's "digital tally", A's formal digital signature and B's formal digital signature are transmitted in order. "Digital tally" is a kind of digital signature but does not satisfy the prescribed format for the format contract. The arbitration functions of the security center are chosen to solve the problems. When intended commitment or unintended human error occurs, "digital tally" is used to prove where and by whom the error has occurred.

CRYPTO-KEY SHARING AMONG MULTIPLE USERS,

T. MATSUMOTO, Department of Electrical Engineering, Faculty of Engineering, University of Tokyo, 7-3-1 Hongo, Bunkyo-Ku, Tokyo 113, Japan, and Y. TAKASHIMA and H. IMAI, Yokohama National University, Japan.

This paper proposes and analyzes a public-key scheme that brings a common crypto-key to each member of a specified group of users. "Registered data" contained in the public file and the "transferred data" exchanged between pairs of members play a significant role in the scheme. The system is based on the commutative and homomorphic properties of power functions over a finite field. Some of its features are as follows:

1. Generation of the key by a non-member is extremely difficult.
2. Different keys can be shared in a fixed group for every data transfer, without updating the publc file.
3. Operation of the scheme is symmetric respective to its various members.
4. The scheme is robust relative to the addition of new gorup members.
5. Since data transfer from different members can occur simultaneously, efficient key sharing is possible, e.g., by spread spectrum techniques.

SECRECY AND AUTHENTICATION: KEY REQUIREMENTS FOR PERFECT SYSTEMS,

PAUL SCHÖBI, The Institute for Signal and Information Processing, Swiss Federal Institute of Technology (ETH), CH-8092 Zurich, Switzerland.

A **perfect secrecy system** according to Shannon is a system where the knowledge of cryptograms does not reduce the uncertainty about the encoded plaintext data for an observer who does not know the secret key. Shannon also gave a relation between the uncertainty about the key and the uncertainty about the encoded plaintext for such systems. A **perfect authentication system** can be defined as a coding system, such that an observer (not knowing the secret key) who wants to produce valid codewords cannot do better than to guess uniformly from all possible codewords (even if he knows a certain number of valid codewords). In this paper, relations among the **numbers of possible** plaintexts, keys and ciphertexts required in perfect secrecy systems and in perfect authentication systems are derived. The following quantities are determined:

1) the minimum key size required for perfect secrecy systems that are secure even if L plaintext/ciphertext pairs are known;
2) the minimum key size required for perfect authentication systems that are secure for all plaintext statistics, when all valid cryptograms are known except one;
3) the minimum key size for systems which provide perfect secrecy **and** perfect authentication when L plaintext/ciphertext pairs are known.

Some constructions are given for perfect secrecy and authentication systems over a large set of parameter values. [Work supported by the Swiss National Fund for Scientific Research.]

CRYPTANALYTIC ASPECTS OF HOMOPHONIC SUBSTITUTION CIPHERS,

DICK E. BOEKEE and JOHAN VAN TILBURG, Delft University of Technology, Dept. of Electrical Engineering, Information Theory Group, P.O. Box 5031, 2600 GA Delft, The Netherlands.

A homophonic substitution cipher, which is actually not a true cipher, assigns to each message symbol, independently of any other message symbol in the message, at random one of the several possible substitution cryptogram symbols. Dunham established a representation theorem which shows that a homophonic substitution cipher is equivalent to an invertible randomization transformation followed by a simple substitution cipher. In this paper the homophonic substitution cipher is described by making use of this representation theorem, and some consequences of this approach are considered. We shall restrict ourselves to the class of Substitution Ciphers (SC), in particular to Simple Substitution Ciphers (SSC) and Homophonic Substitution Ciphers (HSC).

NOTES

SESSION WA3

CODING TECHNIQUES

ON A REDUNDANCY CONTROL BY A DISCRETE COSINE TRANSFORM,

KOHJI MOTOISHI, Department of Computer Science and Communication Engineering, Kyushu University, 6-10-1, Hakozaki, Higashiku, Fukuoka 812, Japan.

A Discrete Cosine Transform (DCT) is generally recognized as one of the best ways to reduce redundancy of acoustic and picture information. The reduced information sequence, however, is not robust against errors which occur during transmission of the information. Under the noisy channel environment, error correcting ability has to be added to the reduced information sequence to be transmitted. The reduced information sequence is, in general, converted to a digital sequence by an AD converter, and encoded in a digital form. This paper presents a method of performing reduction of redundancy and addition of error correcting ability in an analog form by using the DCT. Specifically, the information sequence is transformed into a frequency-domain sequence by the DCT. Some higher-degree elements of the sequence are removed and zeros are packed instead. This frequency-domain sequence is re-transformed into a data-domain sequence by the Inverse Discrete Cosine Transform and is transmitted. Without the expense of excessive elements, the sequence has error correcting ability $[m/2]$, $[\cdot]$ being Gauss's symbol.

BLOCK-CONVOLUTIONAL CODES AND THRESHOLD REPEATED DETECTION ALGORITHM OF WRITE-ONCE MEMORY,

SHI YI SHEN, Department of Mathematics, Nankai University, Tianjin, People's Republic of China.

In this paper, we give an encoding and decoding algorithm for write-once memories using well known block-convolutional codes and a threshold repeated detection decoding method developed by the author in 1982. The algorithm has the following properties

i) The coding is easy to compute (i.e., the complexity of encoding and decoding is a polynomial algorithm in time and memory).

ii) The code rate approaches 1.680, and the error can be made arbitrarily small.

The author thinks that there exists a possibility of using the coder for rewriting information on the write-once memory.

ON d_{FREE} OF ORCHARD CODES,

SPIRA MATIĆ, DJORDJE I. JANKOVIĆ, and VOJIN E. ZIVOJNOVIĆ, "Boris Kidric" Institute - Vinca, Computer Systems Design Lab., Dept. 270, POB 522, 11001 Beograd, Yugoslavia.

Orchard codes are high rate systematic, linear tree codes with rate $R = (n-1)/n$. The minimum distance of an orchard code can be determined from the corresponding parity check matrix, which readily follows from the coding pattern. We used several structural properties of orchard codes to estimate d_{free}. We found that the following relation holds: $d_{free} = d_{\min} + g(n)$, where $g(n)$ is an integer function of the number of rows in the coding pattern of the corresponding orchard code.

CONVOLUTIONAL CODES ON TIME-VARYING CHANNELS,

P. PIRET, Philips Research Laboratory, 2,av. Van Becelaere, B-1170 Brussels, Belgium.

The compound distance profile is introduced as a quality criterion of a convolutional code used on a memoryless compound channel. This concept is illustrated by some constructions of convolutional codes having a strong algebraic structure. This concept is then refined to take into account the possibility of unequal error protection.

ON TERNARY ERROR CORRECTING LINE CODES,

H.C. FERREIRA, J.F. HOPE, and A.L. NEL, Faculty of Engineering, Rand Afrikaans University, Laboratory for Cybernetics, P.O. Box 524, Johannesburg 2000, South Africa.

In this paper we investigate the development of ternary line codes which have certain error correction capabilities. These line codes also can be used in input restricted channels such as the metallic cable systems employed by pulse code modulation schemes.

Markov diagrams are given for sources generating ternary sequences satisfying various restrictions on maximum runlengths, digital sum variation and transitions between extreme signal levels. Extensive tables with the numerical values of the capacities in bits/symbol are presented for the corresponding input restricted channels.

We derive Gilbert type lower bounds on the minimum Hamming and Euclidean distances achievable by nonlinear or linear ternary block codes of rate lower than the channel capacity and satisfying the input restrictions. These bounds can be tightened for dc free codes.

Finally, the results of exhaustive computer searches for sets of ternary single symbol error correcting code words of various word lengths are tabulated. Most important of these codes, is a 12B12T code which is compatible with the 1B1T HDB3 systems.

SESSION WA4

SOURCE CODING II

EMPIRICAL BAYES ADAPTIVE DECODING FOR SOURCES WITH UNKNOWN DISTRIBUTION,

HELIO MAGALHAES DE OLIVEIRA, Coordenação do Mestrado em Engenharia Elétrica, Departamento de Eletroônica e Sistemas, CTUFPE, Cidade Universitária, 50.000, Recife-PE, Brazil.

A decoding algorithm for sources with unknown distribution is presented, which uses adaptive decision thresholds. The method is based upon a decision-directed receiver and on results derived from the empirical Bayes unsupervised learning technique, being appropriate for channels with low SNR. The algorithm's convergence is analyzed and it is shown that the decoding error probability almost surely converges for the value that would be obtained if the source prior distribution were known. An application for binary transmission with digital modulation is discussed and the association of the technique with linear block codes is considered. This results in an adaptive MAP decoding procedure for such codes.

ESTIMATION VIA ENCODED INFORMATION,

ZHEN ZHANG and TOBY BERGER, Center for Applied Mathematics and School of Electrical Engineering, Cornell University, Ithaca, NY 14853, USA.

We extend some results from classical estimation theory to the case in which the observations must be communicated to the point at which the estimate is generated. Particular emphasis is placed on extending Cramer-Rao theory to determine how the minimum variance of an unbiased estimator depends on the communication rates. Explicit results are given for Gaussian sources. [This work was partially supported by NSF Grant ECS-8305681.]

ROBUST ADAPTIVE BUFFER-INSTRUMENTED ENTROPY-CODED QUANTIZATION OF STATIONARY SOURCES,

J.W. MODESTINO, R.J. SHELDON, Electrical, Computer and Systems Engineering Department, Rensselaer Polytechnic Institute, Troy, NY 12180, USA, and N. FARVARDIN, Electrical Engineering Department, University of Maryland, College Park, MD 20742, USA.

Entropy-coded quantization of stationary memoryless sources is known to provide a relatively efficient source encoding technique in a rate-distortion sense. However, transmission of the resulting variable-length codes over a fixed-rate channel necessitates the use of a buffer of finite, and preferably small, size. This requirement, in turn, results in the problem of buffer management. The probability of eventual buffer underflow or overflow is unity without some form of buffer-instrumented adaptive feedback control. This paper investigates the effects of various source statistics and buffer management algorithms for a buffer of fixed size and describes an algorithm that provides particularly robust rate-distortion performance for a wide range of stationary sources. The performance of this scheme is compared to conventional adaptive pulse code modulation (APCM) operating at the same fixed channel transmission rate. [This work was supported in part by ONR under Contract N00014-75-C-0281.]

SEQUENTIAL UNIVERSAL ENCODING OF INDIVIDUAL MESSAGES,[+]

YU. M. SHTARKOV,

No Abstract Available

[+]Denotes Long Paper

SESSION WA5

DETECTION THEORY II

A TWO THRESHOLD FSS TEST FOR MULTIPLE HYPOTHESES,

S. FLEISHER and H. SINGH, Technical University of Nova Scotia, Halifax, Nova Scotia, and E. SHWEDYK, University of Manitoba, Winnipeg, Manitoba, Canada.

A sequential procedure for testing multiple hypotheses with different means/variances is developed. The method constitutes a two-threshold (TT) test for fixed-size packages of samples with a sequential procedure of discarding the package for which no decision is reached, and subsequently testing a new package. The objective is to find an optimum package size N_o which leads to the minimum overall Average Sample Number (ASN) for a given overall error probability.

An optimization algorithm is developed to make possible the application of the procedure.

It is shown for the M-ary, different means/variances cases, that for error rates $\leq 10^{-6}$, the number of samples required by the TTFSS test is, on the average, approximately half that needed by a Fixed Sample Size (FSS) test, but, as expected, somewhat more than the ASN obtained with a conventional sequential test. With decreasing error probabilities, the TTFSS test performance approaches that of conventional sequential methods.

LIKELIHOOD-RATIO TESTS FOR NARROW-BAND STRUCTURE,

DAVID J. THOMSON, AT&T Bell Laboratories, Murray Hill, NJ 07974, USA.

This paper introduces a likelihood ratio test for the presence of spectral structure in a narrow band from a short sample of a process. Under the null hypothesis that the spectrum within the bank $(f - W, f + W)$ is locally white an explicit bandlimited predictor can be constructed using Slepian sequences. Under the alternative hypothesis a similarly bandlimited model is constructed from the data using a multiple-window variant of the Chao-Gilbert autoregressive procedure. The test is given by the ratio of the two likelihoods.

Under the additional assumption that the band of interest contains periodic signals, parameters may be estimated by a combination of conventional and multiple-window methods.

An advantage of the multiple-window modifications is that the estimates may be "jackknifed" to reduce bias and estimate uncertainties in the parameters without *a priori* knowledge of the signal-to noise ratio.

MULTI-DIMENSIONAL QUANTIZATION FOR MINIMAL ASYMPTOTIC PROBABILITY OF ERROR,

JAMES A. BUCKLEW and G. BENITZ, Electrical and Computer Engineering Dept., University of Wisconsin-Madison, Madison, WI 53706, USA.

In many applications it is necessary to digitize data before performing a maximum-likelihood test. In this case, the power of the test is the desired performance criterion. From a result of Chernoff, it is possible to look at the asymptotic rate at which the probability of error vanishes. This error rate is minimized over a class of multi-dimensional quantizers, assuming a large number of quantization levels.

THRESHOLD VECTOR FIELD DETECTORS,

DAVID MIDDLETON, 127 East 91st Street, New York, NY 10128, USA.

This paper extends the recently developed canonical treatment of threshold signal detection in non-Gaussian scalar noise fields to vector signal and noise fields. New optimum and suboptimum algorithms are obtained, based on the first-order pdf's of the general vector field, along with associated performance measures, for the three modes of detection: (i) coherent; (ii) incoherent; and (iii) composite detection (= (i) + (ii)). The specific structure of the bias term needed to ensure both Bayes local optimality (LOB) and asymptotic optimality (AO) are given, along with the auxiliary statistics of the algorithm, required for performance evaluation. In contrast to the "classical" scalar cases, these new algorithms, as expected, are more complex but can lead to additional reduction in the minimum detectable signal. Some numerical examples are noted, as well as general structural and statistical differences between the earlier scalar and present vector formulations. [This work was supported under Contract N00014-84-C-0417 with the Office of Naval Research, Code 1111SP.]

ON DETECTION OF NUMBER OF SIGNALS IN PRESENCE OF SPATIALLY COLORED NOISE USING INFORMATION THEORETIC CRITERIA,

L.C. ZHAO, P.R. KRISHNAIAH, and Z.D. BAI, Center for Multivariate Analysis, University of Pittsburgh, Pittsburgh, PA, USA.

Consider the model

$$\underline{x}(t) = A\underline{s}(t) + \sqrt{\lambda}\underline{n}(t)$$

where $\underline{x}(t)^T = (x_1(t), \ldots, x_p(t))$, $\underline{s}^T(t) = (s_1(t), \ldots, s_q(t))$, $A = (\underline{A}(\phi_1), \ldots, \underline{A}(\phi_q))$, $\underline{s}(t)$ and $\underline{n}(t)$ are complex independent, zero mean, Gaussian, with covariance matrices Ψ and Σ_1 respectively. Each $s_i(t)$ is a waveform referred to as the i^{th} signal, λ is a constant, and $A(\phi_i)$ is a complex vector depending on the unknown parameters of $s_i(t)$. Let λ_i, $1 \leq i \leq p$ denote the eigenvalues of $\Sigma_2\Sigma_1^{-1}$ where $\Sigma_2 = A\ \Psi\ A^{\cdot} + \lambda\Sigma_1$, and $A^{\cdot}$ is the transpose of the complex conjugate of A. The number of signals transmitted is equivalent to the number of eigenvalues of $\Sigma_2\Sigma_1^{-1}$ which are different from the smallest eigenvalue.

We review methods on estimation of the number of signals transmitted when an estimate of Σ_1 is available and λ is known or unknown. One method (Rao, "Likelihood ratio tests for relationships between two covariance matrices," *Studies in Econometrics, Time Series and Multivariate Statistics,* Academic Press 1983) consists of deriving a likelihood ratio test and a modified likelihood ratio test, as λ is known or unknown. Another method (Zhao, Krishnaiah, Bai, (1986),"On detection of the number of signals with arbitrary noise covariance matrix," *Journal of Multivariate Analysis)* uses an information theoretic criterion and provides strongly consistent estimates.

NOTES

SESSION WA6

SEQUENCES I

COMPLEX SEQUENCES CHARACTERIZED BY A TWO-VALUED PERIODIC AUTOCORRELATION FUNCTION,

JOHN H. COZZENS, The MITRE Corporation, Bedford, MA 01730, USA.

Let p be a prime, α a primitive element for Z_p and ω a primitive root of unity mod $p-1$. For each $k \geq 0$ ($k > 0$), the mapping Ξ_k: $Z_p^* \rightarrow C$ defined by $\Xi_k(m) = \omega^{k \log_\alpha(m)}$ is a group homomorphism called a *(nonprincipal) character* mod p. Scholtz and Welch have shown that for nonprincipal Ξ_k, the induced character sequences $\Xi_k = (0, \Xi_k(1), \ldots, \Xi_k(p-1))$ have almost ideal periodic autocorrelation properties, namely, $P_{\Xi_k \Xi_k}(\tau) = -1$ for $\tau > 0$ and $P_{\Xi_k \Xi_k}(0) = p-1$. In a different direction, McKay and Wang have shown that for arbitrary n, the autocorrelation equation $P_{x,x}(\tau) = -1$, $\tau > 0$ and $P_{x,x}(0) = n-1$ has a solution x with $x_i \in \{0, \pm 1\}$ if and only if n is prime, in which case x is (up to cyclic shifts and multiplication by -1) the character of order 2, or in more familiar terms, a Legendre sequence. This talk will describe recent progress toward proving a conjecture based on these results, namely, for ς a primitive $\phi(n)^{th}$ root of unity and k a divisor of $\phi(n)$, $P_{x,x}(\tau) = -1$, $\tau > 0$ and $P_{x,x}(0) = n-1$ has a solution x with $x_i \in \{0, \varsigma^{nj/k} \mid 0 \leq j < \phi(n)\}$, if and only if n is prime, in which case x is a nonprincipal character mod p having order k (i.e., the smallest $k > 0$ for which $x^k = \Xi_0$). The relationships to and the implications of such a characterization to problems in analytic number theory, sequence design, familiar combinatorial structures including singly periodic Costas arrays and graph labelling will also be discussed.

CYCLOTOMIC SEQUENCES AND CYCLIC CODES,

R.M. CAMPELLO DE SOUZA, Departamento de Eletronica e Sistemas - CT, UFPE - Cidade Universitaria, CEP: 50.000 - Recife - PE - Brazil.

A family of binary sequences is introduced through which an efficient algorithm for finding the roots of polynomial idempotents over $GF(2^m)$ is obtained. The method is based upon the properties of the Galois Field Transform (GFT) and has some interesting applications to cyclic codes. Two such applications in the context of decoding are discussed and it is shown that the root-finding method is indeed a fast way of computing the inverse Fourier Transform over a finite field as well as the roots of the error locator polynomial.

m-SEQUENCES OVER $GF(q)$ AND $GF(q^m)$,

WILLIAM J. PARK and JOHN J. KOMO, Electrical and Computer Engineering, Clemson University, Clemson, SC, USA.

Relationships between m-sequences over $GF(q^m)$ and $GF(q)$ are developed which show that m-sequences over $GF(q^m)$ can be obtained directly from m-sequences over $GF(q)$. This then enables the generation of m-sequences over $GF(q^m)$ of length $q^{nm}-1$ (corresponding to degree n primitive polynomials in $GF[q^m,x]$, the set of all polynomials with coefficients in $GF(q^m)$) from known m-sequences over $GF(q)$ of length $q^{nm}-1$ obtained from degree nm primitive polynomials in $GF[q,x]$. These m-sequences over $GF(q^m)$ then have better autocorrelation properties than equal length m-sequences over $GF(q)$. Each of the elements of the m-sequence over $GF(q^m)$ is a vector expressed as a linear combination of elements from $GF(q)$ times a set of basis elements for $GF(q^m)$ over $GF(q)$. For $m=2$ the m-sequence over $GF(q^2)$ is given as a shifted version of an m-sequence over $GF(q)$ times the first basis element plus the same m-sequence over $GF(q)$ shifted a different amount times the second basis element. It is also shown that when the set of all primitive polynomials of degree mn in $GF[q,x]$ is factored in $GF[q^m,x]$ occurs exactly once as one of these factors. This fact then enables all of the primitive polynomials in $GF[q^m,x]$ to be obtained from a complete set of the primitive polynomials in $GF[q,x]$ via the corresponding m-sequences.

A GENERAL CLASS OF WINDMILL POLYNOMIALS FOR FAST M-SEQUENCE GENERATION,

BEN SMEETS, Department of Computer Engineering, University of Lund, P.O. Box 118, S-221 00, Lund, Sweden.

The windmill technique is an attractive alternative to the Lempel-Eastman technique for fast m-sequence generation. In this paper we generalize the class of linear recurrence relations for which the windmill technique results in an m-sequence generator. Furthermore, a converse is given to a set of known necessary conditions, i.e., if $\alpha(t) = 1 - \sum_{i=1}^{m} \alpha_i t^i$ is the feedback polynomial of the s vanes of the windmill, $f(t) = \alpha(t^s) - \beta t^n$ is a ML-polynomial over $GF(q)$ of degree n, $ms < n$, and gcd $(n,s) = 1$, then there exists a windmill machine that generates an m-sequence of period q^n-1, s times as fast as a linear feedback shift register with feedback polynomial $f(t)$.
This work partially supported by the National Swedish Board for the Technical Development, Grant 85-3759, University of Lund.

A UNIFIED DERIVATION OF CONDITIONS FOR THE EQUIDISTRIBUTION OF TLP SEQUENCES GENERATED BY *M*-SEQUENCES,

K. IMAMURA and S. MATSUFUJI, Department of Electrical Engineering, Saga University, Saga, 840, Japan.

Let $\{a_i\} = \{tr(\beta\alpha^i)\}$ be an m-sequence over $GF(q)$ of period $T = q^n - 1$, where $\beta \in GF(q^n)$, α is a primitive element of $GF(q^n)$, and $tr(\ )$ denotes the trace over $GF(q)$. The TLP sequence $\{w_i\}$ generated by $\{a_i\}$ is the L-tuple sequence of period T defined by $w_i = (a_i, a_{i+\tau_1}, \ldots, a_{i+\tau_{L-1}})$. The TLP sequence $\{w_i\}$ is said to be k-distributed $(k \leq n/L)$ if, in the one period of the kL-tuple sequence $\{(w_i, w_{i+1}, \ldots, w_{i+k-1})\}$ $(0 \leq i \leq T-1)$, each kL-tuple over $GF(q)$ appears q^{n-kL} times, with the exception of the zero kL-tuple which appears $q^{n-kL} - 1$ times. The k-distributivity is desirable when we use $\{w_i\}$ as a pseudorandom sequence. This paper presents the following fundamental theorem: **Theorem**: $\{w_i\}$ is k-distributed if and only if the kL elements in the set $\{\alpha^{\tau_i+j}, 0 \leq i \leq L-1, 0 \leq j \leq k-1\}$, $(\tau_0 = 0)$ are linearly independent over $GF(q)$. From the above Theorem all of the known results (e.g., Fushimi and Tezuka, Comm. ACM, 1983) can be easily derived by showing that the set $\{\alpha^{\tau_i+j}\}$ or its equivalent becomes a subset of a polynomial basis of the form $\{1, \gamma, \ldots, \gamma^{n-1}\}$ for $GF(q^n)$. In case of $k = 1$ and $\tau_j = j\tau$ $(1 \leq j \leq L-1)$ the condition in the above Theorem reduces to a simple one such as $q\tau, \ldots, q^{L-1}\tau \not\equiv \tau \ (mod\ T)$, which is independent of $\{a_i\}$ used to generate $\{w_i\}$.

PLENARY LECTURE

TRELLIS CODING WITH EXPANDED SIGNAL SETS — AN OVERVIEW,

GOTTFRIED UNGERBOECK, IBM Zurich Research Laboratory, 8803 Rüschlikon, Switzerland.

Binary convolutional coding and modulation with soft Viterbi decoding has since long been established as a power-efficient technique for transmission at information rates <2 bit/sec/Hz (one-sided). More recently, trellis-coded modulation with expanded signal sets extended this concept into the regime of power- and bandwidth-efficient transmission at rates ≥ 2 bit/sec/Hz, where M-ary modulation ($M > 2$) must be employed. The common factor in both cases is the joint optimization of coding and modulation functions to achieve large free Euclidean distance between coded signal sequences.

In the case of binary modulation (or four-phase modulation, i.e., two binary modulations in quadrature), Hamming distance and squared Euclidean signal distance are equivalent, and hence well-known binary codes are directly applicable and sufficient. For M-ary modulation this equivalence no longer exists. Coding theory seemed to remain unsuccessful in this area for a long time. It was felt, e.g., in the voiceband modem industry, that the coding gains achievable by error-correction coding on top of M-ary modulation with hard-decision demodulation could not justify the resulting bandwidth expansion or data-rate reduction. The problem was finally overcome by providing redundancy for coding in the form of signal-set expansion and showing that trellis codes can be designed directly for optimum Euclidean distance without reference to Hamming distance. Thus, coded modulation schemes were found which achieve coding gains of 3 - 6 dB without bandwidth expansion or data rate reduction, when compared to uncoded modulation. The concept was quickly adopted by industry, and is now becoming widespread.

In the Lecture, the general principles of trellis-coded modulation for transmission of m information bits per modulation interval are reviewed. A binary convolutional encoder is used to expand m bits into $m + 1$ bits which are then mapped by the modulator into a signal of an expanded set of 2^{m+1} signals. Partitioning of the signal set into subsets with increasing intra-subset distances plays a central role. It defines the signal mapping used by the modulator, and provides a tight bound on Euclidean distance which permits an efficient search for optimum codes. For larger values of m, only $k < m$ bits participate in convolutional encoding. The $k + 1$ encoded bits select one subset out of 2^{k+1} subsets, and the remaining $m - k$ uncoded bits indicate the signal within this subset to be transmitted. Following this general discussion, questions concerning carrier-phase sensitivity and code symmetry under phase rotations in the case of carrier modulation are addressed. The achievement of 90°-phase symmetry by nonlinear trellis codes is shown. The concept of trellis-coded modulation is finally extended to schemes which use signal sets of higher dimensionality. The partitioning of these signal sets reveals a high degree of structure. From the resulting intra-subset distances, the optimum trellis codes can be readily determined. Connections with block codes based on the densest lattices become visible, and new possibilities to construct phase-symmetric codes are found.

SESSION THA1

ALGORITHMS AND COMPLEXITY

IMPROVED FREDMAN-KOMLOS BOUNDS FOR PERFECT HASHING VIA INFORMATION THEORY,

J. KÖRNER and K. MARTON, Mathematical Institute of the Hungarian Academy of Sciences, Budapest, P.O.B. 127, H-1364, Hungary.

A set of sequences of length t which form a b-element alphabet is called k-separated if for every k-tuple of the sequences there exists a coordinate in which they all differ. The problem of finding, for fixed t,b and k, the largest size $N(t,b,k)$ of a k-separated set of sequences is equivalent to finding the minimum size of a (b,k)-family of perfect hash functions for a set of a given size. We shall improve the bounds for $N(t,b,k)$ obtained by Fredman and Komlos [*Siam J. Algeb. and Disc. Methods*, Vol. 5, pp. 61-68, 1984].

Korner has shown that the proof in Fredman and Komlos can be reduced to an application of the sub-additivity of graph entropy. He also pointed out that this subadditivity yields a method to prove non-existence bounds for graph covering problems. We have established a new non-existence bound by an extension of graph entropy to hypergraphs:

Theorem

For fixed b and k, and asymptotically in t,

$$\frac{1}{t}\log N(t,b,k) \lesssim \min_{0 \le j \le k-2} \frac{b(b-1)\ldots(b-j)}{b^{j+1}} \log \frac{b-j}{k-j-1} .$$

Besides we show

$$\frac{1}{t}\log N(t,3,3) \gtrsim \frac{1}{4}\log \frac{9}{5},$$

a result proving that (simple) random choice is not optimal for finding large 3-separated sets.

COORDINATION COMPLEXITY AND THE RANK OF BOOLEAN FUNCTIONS,

B. GOPINATH and VICTOR K. WEI, Bell Communications Research, 435 South Street, Morristown, NJ 07960, USA.

A (generalized) Boolean function is a mapping from binary n-tuples to subsets of binary n-tuples. We study the decomposition of Boolean functions into smaller blocks. The smallest possible Boolean functions are called atoms. The rank of a Boolean function is the logarithm of the minimum number of tensor products of atoms that sum up to it. The rank is a measure of the coordination complexity in a distributed computing environment. In the execution of a joint task, the minimum number of bus lines required for coordinating an array of concurrent processors equals the rank. Methods of combining Boolean functions are studied, and the ranks of many well-known functions such as AND, OR, XOR, COMPARATOR, ... etc., are determined. In particular, the rank of the ADDER is found to be n log3.

COMMUNICATION COMPLEXITY,

ALON ORLITSKY and ABBAS EL GAMAL, Information Systems Laboratory, Dept. of Electrical Engineering, Stanford University, Stanford, CA 94305, USA.

The communication complexity of a function $f: \{1, \ldots, n\} \times \{1, \ldots, n\} \rightarrow \{0,1\}$ is the number of information bits two processors need to exchange in order to compute $f(x,y)$ when, initially, one knows x and the other knows y.

Tight bounds on all bounded-error complexity measures of most functions are provided. It is shown that the complexity measures fall into two classes. For every $n \leq s \leq n^2/2$, most functions with s ones have:

- worst-case error-free complexities (deterministic or randomized) of about $\log n$ bits
- average error-free and worst-case ϵ-error complexities of only about $\log \frac{s}{n}$ bits.

The difference between the classes ranges up to exponential (for space functions) but for most functions (since they have about $n^2/2$ ones) the two classes coincide.

AN OBSERVATION ABOUT DES,

SALIGRAM SHIVA, Department of Electrical Engineering, University of Ottawa, Ottawa, Ontario, K1N 6N5 Canada.

As is well-known, every round of the DES algorithm involves the mapping of a 32-tuple into a 32-tuple through substitution boxes. With $a_0'a_1'a_2'a_3'$ as any 4-tuple, let σ_1 represent the 32-tuple $a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'a_0'a_1'a_2'a_3'$. We demonstrate that, under the 48-bit key obtained by repeating the 6-tuple $a_3'a_0'a_1'a_2'a_3'a_0'$ eight times, both σ_1 and σ_2 map into the 32-tuple 11000001010100101111110101010110.

ARITHMETIC OPERATIONAL ALGORITHMS FOR VARIABLE-LENGTH DATA ENCRYPTION,

HISASHI SUZUKI and SUGURU ARIMOTO, Faculty of Engineering Science, Osaka University, Toyonaka, Osaka, 560 Japan.

An efficient method of data encryption is proposed with arithmetic operational algorithms. The length of input data sequences to the encoder is fixed in ordinary methods, but not fixed in our method, which causes great confusion for cryptanalyzers. The encryption of a binary data sequence is executed recursively by dividing a set of candidates of output sequences into two subsets labeled by binary symbols and regarding the subset that corresponds to a data component as the new set, and finally by selecting an output sequence. Here the patterns of division depend on a sequence of random numbers called the key. A legal user who knows the key can reproduce the data sequence by simulating the encryption, while an illegal user who does not know the key cannot. It is shown that the transmission efficiency approaches the theoretical upper bound, by controlling appropriately the patterns of division, and that the exponent of the number of patterns of division that should be examined in exhaustive cryptanalysis is $O(2^n)$, where n denotes the length of the encrypted output sequence in encryption.

SESSION THA2

SOURCE CODING III

DISTRIBUTED VECTOR TRELLIS CODING OF NOISY SOURCES,

ENDER AYANOĞLU and ROBERT M. GRAY, Information Systems Laboratory, Department of Electrical Engineering, Stanford University, Stanford, CA 94305, USA.

Simulation results for low rate vector trellis waveform coding of random waveform sources with additive and statistically independent noise are presented. It is assumed that one only has access to noisy samples from a given source and aims to compress the original source samples in the sense of minimizing the statistical average of a distortion measure between the actual source and its reproduction using a fixed transmission rate. The design is based on a training sequence of the noisy samples and consists of using a modified distortion measure with a code design algorithm. Results for an equivalent two-step approach are compared with distortion-rate theory bounds.

The code design algorithm is modified for the design of quantizers cooperating to compress a random source in a distributed context. Since distortion-rate theoretical results are not available, comparisons are made with an equivalent complexity, optimal, centralized quantizer of similar structure with access to the same observations. [This work was partially supported by DARPA/NAVELEX Contract N00039-84-C-0211 and by the National Science Foundation.]

RIGHT-LEANING TREES WITH A PSEUDO-HUFFMANIAN LENGTH,

HERMAN AKDAG and BERNADETTE BOUCHON, Université Paris VI - Tour 45, 4, place Jussieu, 75252 Paris Cédex 05, France.

Methods to construct binary trees with an optimal length either work from the leaves to the root (Huffman algorithm) or give an approximately minimal length. We study an algorithm based on the construction of right-leaning trees (with non-decreasing ranks and non-increasing probabilities from the left to the right) which processes from the root to the leaves and yields the same length as Huffman trees, for well-determined classes of probability distributions associated with the events corresponding to the leaves. In the other cases, the length of the trees constructed in such a way is very close to the Huffmanian length.

REDUNDANCY AND COMPLEXITY ASPECTS FOR ARITHMETIC CODES,

TJALLING J. TJALKENS and FRANS M.J. WILLEMS, Eindhoven University of Technology, Dept. of Electrical Engineering, Den Dolech 2, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

Arithmetic source codes were described by Rissanen and Langdon. Pasco also invented algorithms based on Elias' fundamental source coding result. In this paper we describe two arithmetic codes both strongly based on Elias' and Rissanen's work. However, we obtain a clear view on the tradeoff between the redundancy or inefficiency of the code

and it's complexity (size and time).

THE LINEAR BOUND ON LINEAR SOURCE CODING,

T.C. ANCHETA, T.J. Watson Research Center, Yorktown Heights, NY 10598, USA.

Let the sequences from a binary memoryless source be compressed by a linear encoder using a compression rate of R output digits per source letter. The minimum average error per digit in recovering the source sequence is shown to be at least $p(1 - R/h)$ where $p \leq 1/2$ is the probability that the source emits the non-zero digit and h is its entropy. Moreover, the quantity $p(1 - R/h)$ is also the lower bound on the minimum per digit error in reconstructing the sequences of a linear code when the codewords carry $(1 - R)$ user digits per channel digit and are transmitted through a binary symmetric channel of crossover probability p. In both systems, equality is achieved with the given bound if and only if $(1 - R/h)$ of the digits are reproduced with an average distortion of p and the rest of the digits are reconstructed with zero distortion.

UNBOUNDED FIBONACCI SEARCH AND RELATED ENCODINGS,

RENATO CAPOCELLI and A. De SANTIS, Dipartimento di Informatica ed Applicazioni, Universita di Salerno, 84100 Salerno, Italy.

In this paper we study Unbounded Fibonacci Searches and associated Encodings. Encoding and Searching are simultaneously considered because of their strong connections.

First, a Uniform Fibonacci Search is introduced, and the relationship of the associated search codes with the Fibonacci numbers is analyzed.

Unbounded Fibonacci Search strategies are then defined. A property of their search codes, namely, the non occurrence in codewords of two consecutive 1's, allows the insertion of a comma between codewords; leading, finally, to synchronizable codes for integers that turn out to be the Lakshmanan code $C(2,11)$; i.e., the set of all binary strings of length greater than 2 in which the pattern 11 occurs only once and as a suffix.

Obviously, the codes considered in the paper are optimal only for some suitable probability distribution. A question which arises is whether they are asymptotically optimal in the sense of Elias. It is shown that all Fibonacci search codes proposed are universal but not asymptotically optimal, that is, the expected codeword length is less than a constant times the entropy of the source, and such a constant cannot approach 1 as the entropy increases.

Some additional properties of Unbounded Fibonacci Searches are also developed. [This work was partially supported by Italian Ministry of Education, Project Progetto ed Analisi di Algoritmi.]

SESSION THA3

RANDOM ACCESS COMMUNICATIONS II

COLLISION RESOLUTION ALGORITHMS FOR SPREAD SPECTRUM ENVIRONMENT,

MICHAEL PATERAKIS and P. PAPANTONI-KAZAKOS, EECS Department, U-157, University of Connecticut, Storrs, CT 06268, USA.

In some spread spectrum environments, the low energy of the transmitted signals, in conjunction with the existence of channel noise, do not allow the distinction between collisions and lack of transmissions. For such environments, and for the Poisson user model, we propose and analyze stable full feedback sensing and limited feedback sensing synchronous transmission algorithms. We assume binary SNS (success versus nonsuccess) feedback per slot, and the possibility of transmission of phony data by a central node. The highest throughput attained by both the full feedback sensing and the limited feedback sensing algorithms is 0.322, although the latter induces somewhat higher delays. This is compensated by the robustness of the limited feedback sensing algorithm in the presence of feedback errors (in contrast to the full feedback sensing algorithm), and its modest requirements on the sensed feedback history. [The work was supported by the ONR, contract N00014-85-K-0547.]

THE STABILITY REGION OF INTERCONNECTED RANDOM ACCESS CHANNELS,

L. GEORGIADIS, L. MERAKOS, and C. BISDIKIAN, Electrical Engineering and Computer Science Department, University of Connecticut, Storrs, CT 06268, USA.

We consider the interconnection of two multiple-access/broadcast networks, each of which connects a large population of bursty users via a packet-switched, broadcast, slotted, collision-type channel. In each network a bridge-node receives internetwork packets from the local users and forwards them to the bridge-node of the other network via a point-to-point link; the bridge-node of the destination network places these internetwork packets in its queue for subsequent broadcasting to the local users. For its broadcast transmissions the bridge-node uses the same random-access channel that the local users use, and, therefore, it participates in the contention. if the external arrival process in network i,$i = 1,2$, is Poisson with intensity λ_i, the stability region of the interconnected system is defined as

$$S = \{(\lambda_1,\lambda_2) \ : \text{ the packet delay is finite with probability one}\}.$$

We develop an analysis method to evaluate a subregion of S, and we give explicit results when the Stack random-access algorithm is used to resolve conflicts at the local level. [This work was supported by ONR, contract NO 662-006.]

AN EXACT ANALYSIS OF A DISTRIBUTED RESERVATION-BASED CDMA SCHEME,

J.E. WIESELTHIER, Naval Research Laboratory, Washington, DC 20375, USA and JULIE A.B. TARR and ANTHONY EPHREMIDES, Electrical Engineering Department, University of Maryland, College Park, MD 20742, USA.

In some applications of radio communications, acknowledgment messages or other feedback information cannot be reliably transmitted. It is useful, therefore, to establish protocols of multiple access that are not based on the availability of feedback messages.

When spread-spectrum signaling is used it is possible to have simultaneous transmissions that do not interfere destructively and that permit the receiver to select which message to monitor. This capability, coupled with the idea of one-way reservations, leads to a multiple access scheme that can operate without transmitter coordination and without feedback from the receiver. This scheme was analyzed before under simplifying approximations. Here we provide a rigorous and exact analysis that yields the achievable throughput. We evaluate the throughput performance for a threshold-based spread-spectrum interference model, although the analysis is applicable to more general (probabilistic) interference models. [Ms. Tarr is an NRL Fellow under ONR Grant N00014-85-0207.]

SPREAD-SPECTRUM RANDOM-ACCESS COMMUNICATIONS WITH MULTIPLE-RECEPTION CAPABILITY,

EVAGGELOS GERANIOTIS and THOMAS KETSEOGLOU, Department of Electrical Engineering, University of Maryland, College Park, MD 20742, USA.

First we examine the performance of a frequency-hopped spread-spectrum multi-receiver, that is, a receiver that can dehop, demodulate and decode simultaneously m distinct frequency-hopped transmitted signals. For frequency-hopped synchronous and asynchronous systems which employ binary or M-ary frequency-shift keying modulation with noncoherent demodulation and Reed-Solomon forward error-control-coding (with errors-only or erasures/errors decoding) the probability of correct reception of l out of m signals (packets) when K signals (packets) are transmitted is evaluated.

Then, the multiple-access capability of this system, which is defined as the maximum number of distinct signals that can be transmitted in the vicinity of the multi-receiver without causing the probability of receiving correctly m signals to fall below a desirable threshold, is computed. Finally, we derive the stable throughput of slotted ALOHA-type frequency-hopped spread-spectrum random-access schemes with retransmission control which employ the multi-receiver described above and investigate the trade-off between throughput and probability of packet error. [This research was supported in part by the National Science Foundation through grant ECS-85-16689 and in part by the Office of Naval Research under contract N00014-86-K-0013.]

THE DELAY DISTRIBUTION OF TREE CONFLICT RESOLUTION ALGORITHMS USING CONSTANT SIZE WINDOW ACCESS,

GEORGE C. POLYZOS and MART L. MOLLE, Department of Computer Science, University of Toronto, Toronto, Ontario M5S 1A4, Canada.

We consider a Random Access protocol for a broadcast communications channel based on a Tree Conflict Resolution Algorithm (TCRA) of the Capetanakis-Tsybankov-Mikhailov type, but in which (constant size) windows on the arrival time axis are used to admit packets into the algorithm, instead of the more common "free" or "blocked" access methods. The system was first proposed by Massey and has maximum stable throughput .43 for the standard TCRA and .46 for the modified algorithm ("level skipping").

We obtain functional equations for the generating functions of epoch length and the delay of a packet in its epoch of successful transmission, as limits of recursive relations for the corresponding metrics of the finite population model obtained. Their solutions come in the form of infinite series. Then, a discrete time $D/G/1$ queueing system with interarrival time the size of the window and service time distribution the generating function of epoch length, provides us the main component of the distribution of the packet delay. Finally, the convolution of the two above components of the delay and the initial delay, which is merely the residual life distribution of the window in which the arrival occurred, gives us the final result, the distribution of packet delay. The exact throughput-delay curve can be obtained by differentiation.

NOTES

SESSION THA4

BANDWIDTH AND SYNCHRONIZATION OF CODES

CONCATENATED CODING SYSTEMS EMPLOYING BANDWIDTH EFFICIENT INNER CODES,

DANIEL J. COSTELLO and ROBERT H. DENG, Department of Electrical and Computer Engineering, University of Notre Dame, Notre Dame, IN 46556, USA.

High speed concatenated coding systems with trellis inner codes and Reed-Solomon outer codes are considered for application in satellite communication systems. Two types of inner codes are studied:

1) High rate punctured binary convolutional codes which result in total effective information rates between 1/2 bit and 1 bit per channel use;

2) Bandwidth efficient signal space inner codes which can achieve total effective information rates greater than 1 bit per channel use.

Two concatenated coding schemes are proposed and analyzed. Scheme 1 is a concatenated coding system without side information. For this scheme, our results indicate that, at decoded BER's between 10^{-6} and 10^{-9}, coding gains from 2 to 7 dB can be achieved with little or no bandwidth expansion and only moderate decoder complexity.

To achieve high reliability decoding, it is advantageous if the inner decoder can provide some reliability information to the outer decoder in the form of soft decisions. Scheme 2 is a concatenated coding scheme with side information. In this scheme, we employ a modified Viterbi decoding algorithm for trellis codes with output reliability information (erasures) and an errors-and-erasures decoder for the Reed-Solomon outer code. If a small percentage of block erasures is allowed ($<1\%$), our results indicate that extremely high reliability (on the order of 10^{-15}) can be achieved, again with little or no bandwidth expansion and a still reasonable decoder complexity. [This work was supported by NASA Grant NAG5-557 and by NSF Grant ECS84-14608.]

A NOVEL CLASSIFICATION OF PHASE CODES,

J.A.S. REDWOOD-SAWYERR, Department of Electrical Engineering, Fourah Bay College, University of Sierra Leone, Freetown, Sierra Leone.

A new classification of modulation schemes from their power spectral densities is proposed using two optimization criteria; the sidelobe rejection factor (RJF), and the slope factor (SLF). By specifying the class of an index set for a given phase code, the performance level is readily implied in terms of sidelobe rejection and the passband slope variation properties.

NODE SYNCHRONIZATION OF $R = 1/2$ BINARY CONVOLUTIONAL CODES,

ANDREA GUBSER and JAMES L. MASSEY, Institute for Signal and Information Processing, Swiss Federal Institute of Technology, CH-8092 Zurich, Switzerland.

Binary rate-1/2 convolutional encoders with code generating-polynomials $G_1(D)$ and $G_2(D)$ are considered where $G_1(0) = 1$. The node synchronization problem is to determine the boundary between the length-two subblocks in the encoded sequence when the receiver enters this sequence at an arbitrary point and observes N consecutive encoded digits. For the noiseless case, it is shown that the probability of synchronization error depends only on the degree of the "unified code-generating polynomial," $G(D) = G_1(D^2) + D \cdot G_2(D^2)$, provided that the encoder is non-catastrophic. The received sequences that are ambiguous in the sense of not uniquely specifying node synchronization are shown in the non-catastrophic case to be the set of all length N output sequences that can be produced by a linear feedback shift-register with connection polynomial $G(D)$. Simulation results for node synchronization error probability when the encoded sequences are transmitted over a binary symmetric channel are used to show that the synchronization performance in the noiseless case is a reliable predictor of performance in the noisy case as well.

OPTICAL ORTHOGONAL CODES,

FAN R.K. CHUNG, JAWAD A. SALEHI and VICTOR K. WEI, Bell Communications Research, Morristown, NJ 07960, USA.

An optical orthogonal code is a family of (0,1)-sequences with good auto- and cross-correlation properties, i.e., the auto-correlation of each sequence exhibits the "thumbtack" shape and the cross-correlation between any two sequences remains low throughout. The study of optical orthogonal codes has been motivated by a problem in the reliable transmission of information over a code-division multiple access fiber optical channel. The use of optical orthogonal codes enables a large number of asynchronous users to send and receive information via a common wide-band communication channel efficiently. The thumbtack-shaped auto-correlation facilitates the synchronization of the desired signal, and the low-profiled cross-correlation reduces interference from unwanted signals. In addition to the optical multiple-access system, optical orthogonal codes also find applications in mobile radio, spread-spectrum communications, radar signal design, and error-correcting codes. In this paper, we shall also discuss methodologies in the design and analysis of optical orthogonal codes with tools including projective geometry, the greedy algorithm, iterative constructions, algebraic coding theory, block design, and various other combinatorial techniques.

ON EFFICIENT SYNCHRONIZATION OF CONVOLUTIONAL CODES,

GROZDAN PETROVIĆ and DUŠAN DRAJIĆ, Faculty of Electrical Engineering, Bulevar Revolucije 73, Beograd, Yugoslavia.

In this paper an efficient synchronization method, based on the trial-and-error approach is presented. The idea is to use only one convolutional decoder with double capacity shift registers, instead of two complete decoders. The proposed decoder functions in the interleaved mode at double speed. The method is illustrated for the case of Massey's diffuse convolutional code with R = 1/2, but it can be easily extended to the convolutional code of any rate.

NOTES

SESSION THA5

QUANTIZATION II

AN OPTIMUM BIT ALLOCATION RULE FOR BLOCK QUANTIZATION,

YOUNG-SERK SHIM and THOMAS S. HUANG, Department of Electrical and Computer Engineering, Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1101 West Springfield Avenue, Urbana, IL 61801, USA.

In this paper, we describe a rule that can optimally allocate bits in the sense that (weighted) mean-squared errors are minimized for the set of k_i-level quantizers ($i = 0,1, \ldots, Q-1$) with Q and k_i's prespecified. The optimality, undominatedness, and uniqueness of the optimum allocation are proved, and the theoretical results are supported by some examples. The algorithm presented has a simple quantizer-like structure, where inputs are the logarithms of component variances and decision levels are simply calculated using the normalized distortion rate function values of an encoder at $b_i = \log_2 k_i$ bits, $i = 0, 1, \ldots, Q-1$. Compared to the results of Huang and Schultheisis (1963) and of Segall (1976), our development relaxes some of their assumptions. It can be seen that Segall's result is a special limiting case of our result.

AN EFFICIENT NEAREST NEIGHBOR SEARCH METHOD,

M.R. SOLEYMANI, Department of Electrical Engineering - H915, Concordia University, 1455 de Mainsonneuve Blvd. W., Montréal, Québec, H3G 1M8 Canada, and S.D. MORGERA, Department of Electrical Engineering, McConnell Engineering Building - Room 514, McGill University, 3480 University S, Montréal, Québec, H3A 2A7 Canada.

The nearest neighbor search problem arises in areas such as pattern classification, nonparametric estimation, and, more recently, in data compression using vector quantization. An algorithm for reducing the computational complexity of nearest neighbor search is given, and simulation results showing its effectiveness for vector quantization is presented. The complexity is reduced by performing a simple distortion test on each codevector, and by avoiding further computation on those which fail it.

The test consists of comparing the absolute error due to each component with the square root of the minimum distortion found so far. Furthermore, while finding the distortion for those codewords which have passed this test, after adding each component's squared error, we check to see if the sum exceeds the minimum distortion found so far or not.

The simulation shows that the approach presented leads to a reduction in the number of multiplications of up to 94% over the conventional method. The number of additions is considerably reduced. The price paid is a moderate increase in the number of comparisons. An additional advantage of this algorithm is the fact that it requires no precomputations and/or extra memory. [This work was supported by Canada Natural Sciences and Engineering Grant A0912 and Québec FCAC Grant EQ 0350.]

VECTOR QUANTIZATION WITH AN AUXILIARY PARTITION,

LUZHENG LU , G. COHEN, and PH. GODLEWSKI, Departement Systèmes et Communications, C.N.R.S., UA 820, Ecole Nationale Supérieure des Télécommunications, 46, Rue Barrault, 75013 Paris, France.

An auxiliary partition, called the nearest vector autocorrelation partition, for substantially reducing the search complexity of a vector quantizers is here proposed. With the correspondence between this auxiliary partition and the original partition of a vector quantizer, the encoding procedure is reduced from a full search through the whole codebook to a full search over a small subset of the codebook. The inside encoding performance is exactly the same, and the outside performance, according to simulation results, is similar to that of the ordinary full search.

AN ALGORITHM FOR SPHERICAL CODES AND QUANTIZERS FROM THE BARNES-WALL LATTICE IN 16 DIMENSIONS,

JEAN-PIERRE ADOUL and CLAUDE LAMBLIN, CRCS, University of Sherbrooke, Québec, Canada.

Spherical codes obtained from a shell of regular lattices are useful for designing modem signal sets and also vector quantizers. The Barnes-Wall regular lattice is the densest known lattice in 16 dimensions. The practical importance of this lattice stems from the facts that it is fairly simple and the number of dimensions is a power of two. Let us call D_n the lattice with integer components in R^n such that the sum of the components is even. The Barnes-Wall Lattice is defined as: $\Lambda_{16} = \cup 2D_n + c_1$ where c_1 is a codeword from the [16,32,8] Reed-Muller code. The points of Λ_{16} fall on spheres of radius $2\sqrt{(2m)}$ for positive integers, $m \geq 2$, thus partitioning the lattice in spherical codes $\Lambda_{16}(m)$. An algorithm is provided for finding the nearest neighbor for some input vector $x \in R^{16}$ within a specified $\Lambda_{16}(m)$. Basically, the algorithm uses the 16×16 Hadamard transform to break the vector into two orthogonal 8-dimensional vectors which can be treated separately using properties of the Gosset lattice E_8. The paper also presents the mean squared error performances versus bit rate when shell m is used for quantizing waveform of iid Gaussian samples.

VECTOR QUANTIZATION OF SPEECH SIGNALS BY ADAPTIVE CODEBOOK ALLOCATION,

H. BREHM and K. TROTTLER, Lehrstuhl für Nachrichtentechnik, Universität Erlangen - Nürnberg, 8520 Erlangen, Cauerstraße 7, West Germany.

It is confirmed that bandlimited speech signals are excellently modelled by spherically invariant random processes (SIRPs). Based on this model rate distortion functions (RDFs) have been calculated, the results of which strongly depend on the type of SIRP under consideration. This performance, however, cannot be confirmed using vector quantization (VQ) schemes operating with only one optimally designed codebook. This is shown by evaluating Gersho's asymptotic bounds to the distortion of a vector quantizer up to a vector length 40.

On the other hand, SIRPs can be considered as mixtures of Gaussian processes with randomly chosen standard deviation. Referring to this representation, a new VQ strategy is analyzed proceeding from an adaptive bit allocation. This allocation scheme is directly related to the evaluation of the RDFs and makes use of the short-time variances of the Gaussian subsources. It is demonstrated that VQ with an adaptive codebook allocation yields a performance, which takes care of variations concerning different SIRP-types. Moreover the rate distortion bounds are reached up to 2 dB even with codebooks at moderate vector lengths. [Parts of this work have been supported by the Deutsche Forschungsgemeinschaft, Bonn, FRG.]

NOTES

SESSION THA6

DETECTION AND ESTIMATION

PERFORMANCE OF A RANDOM THRESHOLD MULTISAMPLE DECISION RULE FOR KNOWN SIGNALS AGAINST A CLASS OF ADDITIVE AMPLITUDE-BOUNDED DEPENDENT NOISE,

JOEL M. MORRIS and CHERRIE C. MALLORY, Electrical Engineering Department, Howard University, Washington, DC 20059, USA.

Results are obtained for the performance of a random threshold multisample decision rule against known signals with additive, unknown-mean, amplitude-bounded dependent noise. This work is proposed as an extension to the performance obtained for a multisample robust decision rule with random interference. The dependent noise sequence is generated by filtering the independent noise sequence using a discrete-time finite impulse response (FIR) filter. Results are depicted in terms of probability-of-error vs. M curves parameterized by N; where M is the number of samples and N is the number of thresholds. The simulated P_e performance results are obtained for a variety of non-Gaussian noise models; (1) Middleton's Class A canonical model; (2) El-Sawy's least favorable noise model; (3) the sum of two Gaussians; and (4) the Rayleigh. Also, the performance of this detector is compared with that of the sign detector against these noise models.

CONFIDENCE INTERVALS BASED ON VERY FEW OBSERVATIONS,[*]

NELSON M. BLACHMAN, Western Division of the GTE Government Systems Corporation, Box 7188-6209, Mountain View, CA 94039, USA.

Confidence limits of the form $\overline{X} \pm tS$ are constructed for the median of a distribution with unknown median and dispersion, where $\overline{X}$ and S are the sample mean and "unbiased" standard deviation based on n observations. Particular attention is given to the values of t needed for the Cauchy and uniform distributions. The latter t suffices for any symmetric unimodal distribution if $t \geq n - 1$. A table compares these values of t for $n = 2, 3, 4$, and 5 with those found by Student for the normal case. This table also includes the cases of $n = 1$, where the confidence intervals are made just wide enough for the least favorable dispersion. The paper concludes with a discussion of the limit for large n, which is Student's t throughout and slightly beyond the domain of attraction of the normal distribution and is smaller elsewhere.

[*]Denotes Long Paper

ON THE DIMENSIONALITY OF DISPLACEMENT SPACES,

HANOCH LEV-ARI, Information Systems Laboratory, Stanford University, Stanford, CA 94305, USA.

The notion of *displacement space* is introduced in the context of adaptive least-squares filtering. The dimensionality of the displacement space determines the complexity of the evolution for the gains of adaptive least-squares *lattice filters.*

Gains of discrete-time adaptive lattice filters have simple evolution equations because the corresponding displacement space is one-dimensional. We show that the same dimensionality characterizes continuous-time adaptive lattice filters that feature a continuous-time gain update. Moreover, such filters can also use a discrete-time gain update procedure, at the cost of increasing the dimensionality of their displacement space (and their complexity) from 1 to $W\tau$, where τ is the time-interval between successive updates, and W is the bandwidth of the signal at the input of the lattice filter.

A NEW TEST IN FACTOR ANALYSIS BASED ON HIGHER POWERS OF THE SAMPLES EIGENVALUES,

S. UNNIKRISHNA PILLAI and FRED HABER, Department of Electrical Engineering and Computer Science, Polytechnic Institute of New York, 333 Jay Street, Brooklyn, NY 11201, USA.

The problem of estimating the number of "systematic" components present in the data is reviewed and in this context a new test based on higher powers of eigenvalues of the sample covariance matrix is derived. The usefulness of this test when the number of systematic components is greater than the dimensionality of the data vector for a certain type of structured covariance matrix is demonstrated.

SESSION THA7

SEQUENCES II

AN INVERSIONLESS ITERATIVE ALGORITHM FOR MULTISEQUENCE SHIFT REGISTER SYNTHESIS,

G.L. FENG and KENNETH K. TZENG, Dept. of Computer Science and Electrical Engineering, Lehigh University, Bethlehem, PA 18015, USA.

A generalization of the Berlekamp-Massey iterative algorithm for multisequence linear feedback shift register synthesis has been previously presented by the authors. Important applications of the generalized algorithm include the decoding of certain cyclic codes up to the Hartmann-Tzeng bound and the Roos bound using multiple sets of syndrome sequences. In this paper, an inversionless version of the generalized algorithm is presented.

SHIFT SEQUENCES OF M-SEQUENCES AND THEIR APPLICATIONS,

AGNES HUI CHAN and RICHARD A. GAMES, The MITRE Corporation, Bedford, MA 01730, USA.

Maximum period linear feedback shift register sequences, commonly called m-sequences, have many applications in modern communication systems. If m is an integer dividing n, then it is well known that an m-sequence of span n can be written as an array in which each column is identically zero or some shift of a fixed m-sequence of span m. These column shifts are used to define a sequence, called the shift sequence, for the m-sequence and the integer m. This paper studies these shift sequences and gives three diverse applications involving them. These applications involve the crosscorrelation properties of m-sequences, a general method of determining the linear span of a class of binary sequences derived from q-ary m-sequences, and a construction of two-dimensional synchronization patterns, called sonar sequences, that have two-dimensional spatial aperiodic autocorrelation functions with minimum out-of-phase values.

FAMILIES OF SEQUENCES WITH OPTIMAL GENERALIZED HAMMING CORRELATION PROPERTIES,

QUANG A. NGUYEN, Technical University of Budapest, 1111 Budapest, Stoczek u.2, Hungary, LASZLO GYORFI, Technical University of Budapest, 1111 Budapest, Stoczek u.2, Hungary, and JAMES L. MASSEY, Institute for Signal and Information Processing, Swiss Federal Institute of Technology, CH-8092 Zurich, Switzerland.

The generalized Hamming correlation function, $H_{xy}(a,i)$, is introduced and defined, for $a \in G$ and $0 \leq i < n$, as the number of positions in which the difference between the component of x and the component of the i^{th} left cyclic shift of y equals a. $H_{xy}(0,i)$ is the conventional Hamming correlation function. The parameter $M(C)$, which is the maximum of the achieved values of $H_{xx}(a,i)$ with $i \neq 0$ and of $H_{xy}(z,i)$ with $x \neq y$, is introduced as a measure of the quality of a family C of n-tuples. This measure is useful in evaluating frequency-hopping sequences and collision-channel protocol sequences.

It is shown that if G has cardinality $|G| = q$ and $M(C) < n$, then $M(C) \geq \max\{\lceil n/q \rceil, \lceil \log_q(n|G|) \rceil\}$. It is then shown that every Reed-Solomon (n,k) code over $GF(q)$ with $n = q - 1$ and $k \geq 2$ contains a subset C of q^{k-2} codewords with $M(C) = k - 1$; this family C is optimal in the sense of meeting the lower bound on $M(C)$ with equality.

BENT FUNCTIONS AND DOUBLY EVEN SELF DUAL CODES,

J. WOLFMANN, GECT, Université de Toulon et du Var, 83130 La Garde, France.

A boolean function of $V = [GF(2)]^n$, n even, over $GF(2)$ is called bent if its Hadamard transform coefficients are all $\pm 2^{n/2}$. The characteristic vector in V corresponding to a bent function is further away from any codeword of the Reed Muller code $R(1,n)$ in the sense of the Hamming distance. Bent functions are used in the construction of the Kerdock codes and also to obtain synchronization binary sequences.

On the other hand binary self dual codes and in particular, those with all weights multiple of 4 (doubly even self dual codes) have been studied extensively and are very important in coding theory.

We establish a link between bent functions and doubly even self dual codes by constructing a one to one mapping from the set of all doubly even self dual codes of length n onto a set of bent functions on V.

GENERALIZED BENT FUNCTIONS -- SOME NEW GENERAL CONSTRUCTIONS AND NONEXISTENCE TESTS,

HABONG CHUNG and P. VIJAY KUMAR, Communication Sciences Institute, Department of Electrical Engineering, University of Southern California, Powell Hall 404, Los Angeles, CA 90089-0272, USA.

This paper contains some new general constructions and existence tests for bent functions and related 2-dimensional dot patterns. Let J_q^m denote the set of m-tuples over the integers modulo q. The first of two simple yet general techniques for constructing one-dimensional ($m=1$) bent functions presented here applies whenever q is of the form, $q = m^n$, (m and n are integers greater than one). The second allows bent functions over J_{mn}^1 to be constructed out of bent functions over J_m^1 and J_n^1 whenever m and n are relatively prime. The graph of a certain class of bent functions (over J_q^1) yields a $(q \times q)$ dot-matrix pattern whose out-of-phase Hamming autocorrelation never exceeds one. The nonexistence proof contained here rules out existence for all even q. Costas arrays correspond to square matrices having one dot per row and one dot per column and an **aperiodic** Hamming correlation whose out-of-phase values never exceed one. Here we investigate rectangular Costas-like arrays whose out-of-phase **periodic** correlation values never exceed one. A previously known construction is cited and a nonexistence test presented. This work was partially supported by NSf Contract ECS-8404281.

SESSION THB1

MULTIDIMENSIONAL CODES

A FURTHER RESULT ON THE GENERALIZED VERSION OF THE CONCATENATED CODES,

SHIGEICHI HIRASAWA, School of Science and Engineering, Waseda University, Tokyo, 160 Japan, MASAO KASAHARA, Faculty of Engineering, Osaka University, Suita 565, Japan, YASUO SUGIYAMA, Faculty of Engineering, Setsunan University, Neyagawa, 572 Japan and TOSHIHIKO NAMEKAWA, Faculty of Engineering, Osaka University.

The generalized version of the concatenated codes has been proposed by the present authors. The code has J Reed-Solomon outer codes with the same length and different rates which are interleaved by an inner code, where the inner code is a nonsystematic code and has J subcodes. Assuming that the inner code is a binary primitive BCH code, the lower bound on the minimum distance of the code is derived and proved to be larger than that of the original concatenated code.

A CASCADED CODING SCHEME FOR ERROR CONTROL,[†]

TADAO KASAMI, TOHRU FUJIWARA, and TOYOO TAKATA, Osaka University, Toyonaka, Osaka, Japan, and, SHU LIN, Texas A&M University, College Station, TX 77843, USA.

In this paper, we investigate a cascaded coding scheme for error control. Error performance is analyzed. If the inner and outer codes are chosen properly, extremely high reliability can be attained even for a high channel bit-error-rate. Several example schemes are studied. One of the example schemes is being considered by NASA for satellite or spacecraft downlink error control.

Portions of this paper were presented at the 8th Conference on Information Theory and Its Applications, Nara, Japan, December 1985. [This research is partially supported by NASA Grant No. NAG 5-407.]

[†]Denotes Long Paper

A GENERALIZATION OF MULTI-DIMENSIONAL PRODUCT CODES,

TAKAHIRO YAMADA, The Institute of Space and Astronautical Science, 6-1, Komaba 4-chome, Meguro-ku, Tokyo 153, Japan.

This paper presents a new class of error correcting codes called generalized multi-dimensional product codes (GMP codes). These codes are a general class of M-dimensional product codes whose codewords are M-dimensional arrays. Generally, GMP codes have higher code rates than the M-dimensional product codes with the same code length and minimum distance. The generator matrix for an M-dimensional GMP code consists of a certain set of rows of the generator matrix for an M-dimensional product code. The product generator codes proposed by W.C. Gore are a subclass of GMP codes. Modified product codes developed by S. Hirasawa et. al. are two-dimensional GMP codes, provided all the column codes for modified product codes are subcodes of one code. The dual code of a GMP code is also a GMP code obtained from the dual codes of the original component codes. A lower bound on the minimum distance of GMP codes is given by a simple formula in terms of the minimum distances of the component codes. An important subclass of GMP codes is a generalized version of the extended generalized Reed-Muller codes.

SESSION THB2

TRELLIS DECODERS

A HYBRID SEQUENTIAL-VITERBI DECODER,

JOHN ASENSTORFER and MICHAEL J. MILLER, South Australian Institute of Technology, Adelaide, Australia.

A decoding scheme for (n,k,m) convolutional codes is described for use with fading channels. The decoder may operate in either a Viterbi decoding mode when the channel is noisy, or a sequential decoding mode when the channel is quiet. As a result, the mean decoding speed of the decoder can be considerably enhanced without significant loss of coding gain.

ERROR BOUNDS FOR *M*-ALGORITHM DECODING OF CHANNEL CONVOLUTIONAL CODES,

C.-F. LIN and J.B. ANDERSON, Electrical, Computer, and Systems Engineering Department, Rensselaer Polytechnic Institute, Troy, NY 12181, USA.

The Viterbi algorithm for the decoding of convolutional codes has been recognized to be a maximum likelihood decoding algorithm. The principal limitation on its practical application is that the complexity of decoding is proportional to the number of encoder states, which itself grows exponentially with the code constraint length K. We pose the following basic question. When the channel SNR is high, is it necessary to keep track of all the encoder states in order to approach the error performance guaranteed by the code's free distance? In earlier work we have investigated this question by testing the performance of a decoder that used the M-algorithm in place of the Viterbi algorithm. The simulation results showed that many fewer retained states are required than the Viterbi algorithm needs. For instance, an 8192-state rate 1/2 code needs only 64 states. In this paper the performance of the M-algorithm is analyzed in terms of some lower bounds. These apply to the hard decision binary symmetric channel. A good, but somewhat complicated bound predicts an error probability vs. SNR curve within 0.5 dB of the simulation results at high SNR. Another approach gives a somewhat looser estimate of the number of paths that need to be retained in order to attain the free-distance error performance, but it is tractable for very long constraint length codes. Some of the practical aspects of this type of decoder are also discussed.

A FRACTIONAL VITERBI-TYPE TRELLIS DECODING ALGORITHM,

TOR AULIN, Chalmers University of Technology, Division of Information Theory, S-412 96 Göteborg, Sweden.

Recent research has shown that efficient and reliable systems for transmission of digital information incorporate the use of a finite memory which can be visualized by means of a trellis. There are systems where the modulation itself can be described by a trellis [1] and there are also systems where the trellis is due to a traditional shift register convolutional encoder connected to a memoryless modulator, with or without the use of a memoryless symbol mapper. The price for improved efficiency and reliability is increased complexity and almost all of it is at the receiver side for optimal reception over a noisy channel.

This complexity is attacked in this work. A Viterbi-type algorithm is analyzed which uses a subset (B) of the number of states (S) in the trellis. The number of states used is fixed, but the subset is chosen dynamically at each step. It is shown that if B is larger than or equal to some value B^*, asymptotic optimality (MLSD over the additive white Gaussian noise channel) is achieved. The new "SA(B)" algorithm is analyzed in detail concerning the processing complexity and a general theoretical model is developed for determination of the detection performance for general trellis codes and different choices of B. [This work was supported by the National Swedish Board for Technical Development Grant 84-3317.]

WEIGHTING THE SYMBOLS DECODED BY THE VITERBI ALGORITHM,

GÉRARD BATTAIL, Ecole Nationale Supérieure des Télécommunications, Departement Systèmes et Communications, 46, rue Barrault, 75634 Paris Cedex 13, France.

It is shown how to modify Viterbi decoding of convolutional codes in order to obtain a reliability estimate of each decoding decision. This enables soft decoding of the outer code in a concatenated system and leads to a significant improvement of the overall performance.

SESSION THB3

MULTIPLE ACCESS COMMUNICATIONS

TIME-HOPPING AND FREQUENCY-HOPPING COMMUNICATIONS,

A.W. LAM and D.V. SARWATE, Department of Electrical and Computer Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, Urbana, IL 61801, USA.

Time-hopping and frequency-hopping multiaccess schemes with error control coding are presented. Such hybrid systems are shown to have excellent throughput performance. Moreover, their normalized throughput is insensitive to the time-hopping (frequency-hopping) strategies when the bandwidth (delay) is large. The *duality* property between time and frequency domains is further explored when we examine systems that can achieve the same throughput either by time-hopping or frequency-hopping alone. For a wide range of channel traffic input rate, we show that the maximum throughput is primarily a function of the code rate and occurs at a code rate of approximately 1/3.

Let l_n^* denote the minimum length of a time-hopping pattern of n elements. The value of l_n^* is known for $n \leq 15$ only, and it is conjectured that $l_n^* \leq n^2$ for all n. By systematically generating time-hopping patterns from simple difference sets, we show that $l_n^* < n^2$ whenever $n-2$ or $n-1$ or n or $n+1$ is a prime power, and that in some instances, our constructions are optimum. Furthermore, we show that $l_n^* < n^2$ for $n \leq 34$ and $l_n^* \leq n^2 + O(n^{1.55})$ for all n. Finally, extensive computations are used to show that $l_n^* < n^2 - n^{1.44}$ for $n \leq 150$. [This research was supported by the U.S. Army Research Office under Contract DAAG29-84-K-0088.]

MULTIPLE-ACCESS CAPABILITY OF FREQUENCY-HOP TRANSMISSION WITH NOISY SIDE INFORMATION,

M.B. PURSLEY, Coordinated Science Laboratory, University of Illinois, 1101 W. Springfield Ave., Urbana, IL 61801, USA.

In previous research (M.B. Pursley, "Frequency-hop transmission for satellite packet switching and terrestrial packet radio networks," *IEEE Trans. on Info. Theory,* Sept. 1986), we investigated the throughput and the packet error probability for frequency-hop transmission in packet-switched radio networks for which there is no background noise and for which perfect side information is available. In practice, of course, the assumptions regarding the noise and side information are only approximately true. These assumptions are relaxed in the present paper, and we consider the performance of a frequency-hop multiple-access packet radio network which has imperfect side information. As in the previous work, the key elements of the communication system are Reed-Solomon coding, slow-frequency-hop signaling, and a method for generating side information concerning the presence or absence of multiple-access interference on the received symbols.

In a system with imperfect side information or background noise, errors-and-erasures decoding is employed. The purpose of the side information is to determine which received symbols are to be erased; however, there is a chance that some symbols with

interference will be missed and other symbols which have no interference will be erased. In the first part of the presentation, we examine the false alarm and miss probabilities that are necessary to provide a prescribed error probability. The second part considers a specific method of generating side information via the transmission of test messages. The effects of the background noise on the side information reliability and the resulting error probability are considered.

A STUDY OF APPROXIMATIONS IN THE ANALYSIS OF DS/SSMA SYSTEMS WITH RANDOM SIGNATURE SEQUENCES,

JAMES S. LEHNERT Purdue University, West Lafayette, IN 47907, USA and M.B. PURSLEY, Coordinated Science Laboratory, University of Illinois, 1101 W. Springfield Ave., Urbana, IL 61801, USA.

Binary direct-sequence spread-spectrum multiple-access communications, an additive white Gaussian noise channel, and a coherent correlation receiver are considered. An expression for the decision statistic is obtained for the case of random signature sequences in terms of a set of mutually independent random variables, and the density function for each random variable in this set is determined. The expression for the decision statistic is used to study the density function for the multiple-access interference and to determine arbitrarily tight upper and lower bounds on the average probability of error. The unique features and advantages of the approach for obtaining bounds are described. Then the bounds are used to study the nature and validity of results obtained using traditional approximations. The effects of transmitter power, the length of the signature sequences, and the number of interfering transmitters are illustrated.

THE CAPACITY REGION OF FREQUENCY-HOP SPREAD-SPECTRUM COMMUNICATION,

MANJUNATH HEGDE and WAYNE STARK, Electrical Engineering and Computer Science Department, University of Michigan, Ann Arbor, MI 48109, USA.

The multiple-access capability of frequency-hop spread-spectrum communication is considered from an information theoretic viewpoint. The model adopted is that of an interference channel with T source-receiver pairs with i^{th} receiver only interested in the message produced by the i^{th} source. Different transmitters use different frequency-hopping patterns which we model as random hopping patterns. We propose some simple models for the resulting channels. We consider both the case where all users are synchronized and the totally asynchronous case. We also consider the cases when the receiver can detect when two or more transmitters hop to the same frequency at the same time. This allows for erasure correction in decoding. Without this information the channel is modeled as a noisy M-ary symmetric channel when there is a hit and a noiseless M-ary symmetric channel in the absence of a hit. For these channel models we determine the capacity region.

SESSION THB4

SYNCHRONIZATION

TIME SYNCHRONIZATION OF FREQUENCY-HOPPED SATELLITE COMMUNICATION SYSTEMS IN THE PRESENCE OF RAYLEIGH FADING,

MARIO A. BLANCO, M/A-Com Government Systems, Inc., Boston Engineering Center, 24 Hartwell Avenue, Lexington, MA 02173, USA.

The problem of uplink time synchronization of frequency-hopped satellite communication systems in a fading environment is considered. A maximum likelihood estimation approach is followed to obtain an algorithm which uses probing signals for coarse epoch estimation. Fine time synchronization is obtained by means of a linear interpolation algorithm. The performance of this estimator is examined for two types of channel fading models: (1) Frequency-selective fading; (2) Flat fading. Diversity techniques to combat the effects of fading and to enhance the acquisition process are also presented. The performance of the time acquisition algorithms combined with frequency and spatial diversity techniques is shown for typical cases of interest. [This work was supported in part by the U.S. Air Force, Electronic Systems Division, under contract F19628-84-C-0056.]

CARRIER TRACKING BY SMOOTHING FILTER CAN IMPROVE SYMBOL SNR,

CARLOS A. POMALAZA-RAEZ, Department of Electrical and Computer Engineering, Clarkson University, Potsdam, NY, USA and WILLIAM J. HURD, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA.

The potential benefit of using a smoothing filter to estimate a carrier phase over use of phase locked loops (PLL) is determined. Numerical results are presented for the performance of three possible configurations of an all-digital coherent demodulation receiver. These are Residual Carrier PLL, Sideband Aided Residual Carrier PLL, and finally Sideband Aiding with Kalman Smoother. The average symbol SNR after losses due to carrier phase estimation is computed for different total power SNRs, symbol rates and symbol SNRs. It is found that smoothing is most beneficial for low symbol SNRs and low symbol rates. Smoothing gains up to 0.7 dB over Sideband Aiding Residual Carrier PLL, and the combined benefit of Smoothing and Sideband Aiding relative to Residual Carrier Loop is often in excess of 1 dB.

A GENERALIZED MODEL FOR MULTI-USER ACQUISITION TO A UHF UPLINK SATELLITE CHANNEL,

MARK BRYAN DURSCHMIDT, Hughes Aircraft Company, Ground Systems Group, Fullerton, CA 92634, USA.

A generalized model for terminal acquisition in a UHF satellite network is presented. Contending terminals obtain network acquisition by sending a probe codeword via the uplink channel and listening for correct reception of the codeword via a pre-established downlink channel. Models are presented which accommodate both a synchronized user environment and an environment in which users have timing offset ambiguity present in their transmitted probing signals. The probe codewords are detected noncoherently using a Code-Division Multiple-Access (CDMA) M-ary signaling technique. A homogeneous Markov chain characterizing a pure death random process models the contention environment. The chain is used to compute the average number of acquired users by using acquisition probabilities which are a function of different numbers of contending users. The model computes user acquisition probability based upon detection test statistics conditional on the presence or non-presence of one additional user to the contention environment.

JITTER ANALYSIS IN A TIMING RECOVERY SCHEME FOR BIPOLAR ENCODED DIGITAL TRANSMISSION SYSTEMS,

ERDAL PANAYIRCI, Istanbul Technical University, Faculty of Electronics and Electrical Engineering, Ayazaga, Istanbul, Turkey.

Assuming the symbol timing circuit consisting of a square-law device followed by a narrow-band filter tuned to the pulse repetition frequency, $1/T$, along with a prefilter for reshaping the pulses entering the timing path, the statistical analysis and the performance evaluation of timing jitter for the bipolar encoded digital transmission systems are investigated. The zero crossings of the nearly sinusoidal timing wave exhibits phase fluctuations known as timing jitter. An expression for the variance of the timing wave is presented. Although this expression is more complex then a statistically-independent data sequence case, it exhibits the same properties for the Fourier analysis under the bandwidth restrictions on prefilter and postfilter characteristics. A condition on prefiltering and postfiltering which gives error-free timing recovery is given. Finally, some numerical examples, provided, show that the rms timing jitter at the periodic zero crossings of the timing wave is negligible and extremely narrow bandwidths for postfilter are not required when some degree of symmetry about $1/2T$ could be achieved.

SESSION THB5

CODING II

A NEW COMBINATORIAL CODING METHOD AND ITS APPLICATION FOR CONSTRUCTING OPTIMAL ERROR-CONTROL CODES,

JIN FAN, Department of Computer Science, Southwestern Jiaotong University, Emei, Sichuan 614202, P.R.C.

In this paper a new coding method based on combinatorial theory is presented. By means of a defined $s(u,v)$ array, the parameters of a (n,k,d) linear code can be determined as $k = C(s,v)$, $n - k = C(s,u)$ and $d = Min(d_1 + 1)$. It is a pleasant surprise that a lot of well-known optimal codes, such as the Golay Code, the Hamming Code and its extensions, a class of BCH Codes and Complex-Rotary Codes may easily be derived from the $s(u,v)$ array without Finite Field theory. This combinatorial method enables us to establish a generalized relation for existing optimal linear codes, and suggests a search program for finding new optimal linear codes.

GENERALIZATIONS OF THE NORMAL BASIS THEOREM,

NADER H. BSHOUTY, Dept. of Computer Science, Technion - Israel Institute of Technology, Haifa 32000, Israel, and GADIEL SEROUSSI, Cyclotomics Inc., 2120 Haste St., Berkeley, CA 94618, USA; on leave from the Dept. of Computer Science, Technion - Israel Institute of Technology, Haifa 32000, Israel.

We present a combinatorial characterization of sets of integers $\{r_0, r_1, \ldots, r_{n-1}\}$, with $0 \leq r_i \leq q^n-2$, such that $\alpha^{r_0}, \alpha^{r_1}, \ldots, \alpha^{r_{n-1}}$ form a basis of $GF(q^n)$ over $GF(q)$ for some $\alpha \in GF(q^n)$. We use this characterization to prove the following generalization of the Normal Basis Theorem: Let $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ be integers in the range $0 \leq \lambda_i < q$, with at most one λ_i equal to zero. Then, there exists an element $\alpha \in GF(q^n)$ such that $\alpha^{\lambda_0}, \alpha^{\lambda_1}, \ldots, \alpha^{\lambda_{n-1}}$ form a basis of $GF(q^n)$ over $GF(q)$. This result, which includes the Normal Basis Theorem as a particular case when $\lambda_0=\lambda_1=\cdots=\lambda_{n-1}=1$, is proved for even q and odd n for all choices of $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ satisfying the above conditions, and for other values of q and n, with restricted sets of values $\{\lambda_i\}$.

ALGORITHM FOR SOLVING QUARTIC EQUATIONS OVER $GF(2^m)$,

N.L. MANEV, Bulgarian Academy of Sciences, Institute of Mathematics, P.O. Box 373, 1090 Sofia, Bulgaria.

A method for solving the quartic equation

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0, \qquad a_i \in GF(2^m) \tag{1}$$

is proposed. The substitution $x = y + \beta$, where β is a root of an appropriate cubic equation transforms (1) into

$$y^4 + a_1y^3 + cy^2 + a_1dy + d^2 = 0.$$

The roots of this equation are the roots of the quadratic equations

$$y^2 + u_iy + d = 0, \qquad i = 1,2$$

where u_1, u_2 are solutions of $u^2 + a_1u + c = 0$ and c and d can be evaluated knowing $a_1,\ldots,a_4$ and β.

This method can be realized with less operations than the one proposed by Chen (IT-28, no. 5, pp. 792-794, 1982).

CONSTRUCTIVE APPROACH TO PRIMITIVE ROOTS,

OSCAR MORENO and CARLOS CARBONERA, Department of Mathematics, University of Puerto Rico, Rio Piedras, Puerto Rico.

Existential problems concerining the primitive roots of finite fields are quite important from a theoretical viewpoint, as well as for applications. Some examples are the recent conjectures (A, B, C, D) of Golomb posing the existence of certain primitive elements over a finite field $GF(q)$, which is of use for the constructions of Costas arrays. In this paper we take a constructive approach to primitive roots and in particular to Golomb's conjecture A.

SESSION THB6

SHANNON THEORY V

A MODIFIED CUTOFF RATE PARAMETER FOR CHANNELS WITH MEMORY,

OFER ELAZAR, Dept. of Electrical Engineering, Technion - Israel Institute of Technology, Technion City, Haifa, 32000, Israel, and AMIRAM KASPI, Israel Ministry of Defense, P.O.B. 2250, Haifa, Israel, and Dept. of Electrical Engineering, Technion - Israel Institute of Technology, Technion City, Haifa, 32000, Israel.

The effect of bit and word interleavers applied to channels with memory on the cutoff rate parameter ($\widetilde{R}_0$) is investigated. Word interleaving is performed by first parsing the channel bits stream into words of k consecutive bits ($k > 1$), and then ideally interleaving the resulting word sequence. It is shown that bit interleaver does not necessarily maximize the cutoff rate, and that for certain channels pair-interleavers, trio-interleavers, etc., may give the highest cutoff rate. The optimum word length varies with channel memory, however, the maximum resulting cutoff rate is only slightly larger than the cutoff rate of the bit interleaved channel.

In order to better utilize the channel memory a modified cutoff rate parameter, $\widetilde{R}_0$, is proposed. $\widetilde{R}_0$ increases with memory size, while preserving all the properties that made R_0 a practical measure of quality for memoryless channels. Lower and upper bounds on $\widetilde{R}_0$ are presented and shown to be tight if channel memory is large enough. In addition, the method developed by Omura and Levitt is applied to channels with memory using $\widetilde{R}_0$ to evaluate an upper bound for the coded error probability of any given convolutional code.

UNION CHERNOFF BOUNDS AND CUTOFF RATE FOR A CLASS OF STATIONARY NON-GAUSSIAN CHANNELS WITH MEMORY,

JOHN S. SADOWSKY, School of Electrical Engineering, Purdue University, West Lafayette, IN 47906, USA.

Performance bounds for a class of stationary channels are considered. Given the history of a "channel state sequence," these channels are time varying and memoryless. Memory is introduced by modeling the channel state sequence as a stationary stochastic process. The model accurately reflects the behavior of many physical communications channels, such as random burst interference, pulsed jamming and multiple user interference. The cutoff rate results presented here are matched to the situation of a random error correcting code. From union-Chernoff bound computations it is demonstrated that this cutoff rate can indicate the sensitivity of ordinary memoryless channel performance analysis with respect to weak channel state dependency. For instance, the parameter may be used to indicate the degree of interleaving which is necessary to break up strong channel state dependency.

BENEFITING FROM HIDDEN MEMORY IN INTERLEAVED CODES,

MORDECHAI MUSHKIN, Elisra Electronic Systems Ltd., 48 Mivtza Kadesh St., Bene Beraq 51203 Israel and, ISRAEL BAR-DAVID, Technion - Israel Institute of Technology, Department of Electrical Engineering, Technion City, Haifa 32000 Israel.

A "bursty" binary channel, having a **normal** and a **disturbed** state, with error probabilities p_0 and p_1, respectively, is modeled using a stationary Markov chain with transition probabilities α (from normal to disturbed state) and β. Code interleaving is frequently used over such channels. Conventional decoders, presuming that the deinterleaved symbols are statistically independent, use decoding algorithms originally designed for memoryless channels, with the disadvantage, however, that the performance of the system is governed by a mean-value error probability $\overline{p} = (p_0\beta + p_1\alpha)/(\alpha + \beta)$.

The decoding algorithm proposed here makes simultaneous use of both the independence of closely located deinterleaved symbols and the residual dependence between appropriate distant ones. The independence of the former enables efficient operation of the error correcting decoder, while the dependence between the latter enables estimation of the channel state that feeds soft-decision variables to the decoder.

THE SOURCE CODING THEOREM AND LARGE DEVIATION THEORY,

JAMES A. BUCKLEW, Department of Electrical and Computer Engineering, University of Wisconsin-Madison, Madison, WI 53706, USA.

This paper gives a proof of Shannon's Source Coding Theorem (SCT) utilizing results from the branch of probability known as large deviation theory. In particular we invoke a result known as Sanov's Theorem which gives rate of convergence information for empirical distributions to obtain our key large deviation lemma. We use this lemma then directly to prove the SCT for Pinsker continuous, ergodic random processes with continuous (but not bounded) distortion measures.

SESSION THC1

APPLICATIONS OF INFORMATION THEORY

ON THE APPLICATION OF INFORMATION-BASED COMPLEXITY TO HUMAN COMMUNICATION,

WALTON B. BISHOP, Department of the Navy, Naval Research Laboratory, Washington, DC 20375-5000, USA.

The semantic problem faced by a human message receiver in determining the meaning of a message resembles the information-based complexity problem, because both deal with information that is partial, contaminated and/or costly. How the human receiver uses the a priori information he or she possess in comprehending a message has long been an enigma for human communication researchers. This a priori information plays an important part in completing messages with missing parts and in correcting errors. However, the a priori information a person possesses must be classified as an "unobservable." This paper shows that this "unobservable", and others related to the human communication process, produce effects that resemble the "indicators" commonly used in social science research. The causal diagram which results from this approach indicates the types of data that should be collected to analyze such elusive parameters as the a priori information possessed by a communicator and the uses made of it. The science classroom is suggested as an ideal laboratory for testing this extension of Shannon theory into the realm of human communication.

EFFICIENT EXHAUSTIVE TESTS BASED ON MDS CODES,

L.B. LEVITIN and M.G. KARPOVSKY, College of Engineering, Boston University, 110 Cummington St., Boston, MA 02215, USA. USA.

Consider a combinational device with m inputs where each output is a Boolean function of at most s binary input variables. The problem of exhaustive testing of such devices can be formulated as follows: construct a binary matrix $T(m,s)$ (rows of $T(m,s)$ are test patterns) with m columns such that all 2^s possible binary vectors appear in each subset of s columns of the matrix. A test with $T(m,s)$ as a test matrix is called s-exhaustive. It is known that there exist s-exhaustive matrices with a number of rows which grows with m as $\log m$ (for any fixed s). However, no constructions are known which satisfy this bound. An iterative procedure for constructing s-exhaustive tests is suggested in which the asymptotic growth of the number of test patterns is arbitrarily close to the theoretical bound. The construction makes use of maximum distance separable (MDS) codes.

Theorem. Let $T(q,s)$ be an s-exhaustive test with N test patterns and $q = p^t$, where p is a prime, and $t=1,2,\cdots$. Then for any k such that $q \geq \lfloor s^2/4 \rfloor (k-1)$ an s-exhaustive test $T(q^k,s)$ can be constructed by use of an MDS code over $GF(q)$ with length

$$n = \lfloor s^2/4 \rfloor (k-1) + 1 \quad .$$

The obtained test $T(q^k,s)$ has nN test patterns.

ASYMPTOTIC NORMALITY OF A MODIFIED ZIV-LEMPEL COMPLEXITY, AND ITS USE AS A NONPARAMETRIC TEST FOR INDEPENDENCE,

PAUL C. SHIELDS, Department of Mathematics, University of Toledo, Toledo, OH 43606, USA.

A binary sequence x_1^M is parsed into nonoverlapping words where the next word is the shortest block not yet seen as a word. To be precise the parsing is defined as follows: $w_i = x_{n_{i-1}}^{n_{i+1}}$, $n_0 = 0$, $n_1 = 1$, and n_{i+1} is the least index n, $n_i < n \leq M$, such that $x_{n_{i+1}}^{n}$ is not one of the w_j, $j \leq i$. This is a slight modification of the well-known Ziv-Lempel parsing algorithm, (IT-23,337-343). Let $W_M = W(x_1^M)$ denote the number of words in our parsing. We show that if (x_n) is generated by unbiased coin-tossing then W_M is asymptotically normally distributed. Only slight changes are needed in Ziv's later paper (IT-24, 405-412) to show that if (x_n) is generated by an ergodic process of entropy-rate H, then $W_M \cdot M^{-1}\log_2 M$ converges almost surely to H. Our result can be viewed as a central limit or second order extension of Ziv's "law of large numbers." Our proof is based on analysis of the random binary tree grown by inserting leaves corresponding to the last bit as each new word is generated. We show that a suitable rescaling of the random vector, which gives the number of words of each length that are available to be the next word, converges weakly to a diffusion process. Our work was inspired by the idea that data compression algorithms implicitly involve tests for independence, for data generated by pure noise cannot be significantly compressed. Thus we would expect that if $\{x_n\}$ is not from an i.i.d. source, then $W(x_1^M)$ will tend to be smaller than $E(W(y_1^M))$, where $\{y_n\}$ is drawn from the i.i.d. process with the same first order distribution as $\{x_n\}$. We report the results of computer studies comparing this test with other standard test procedures, such as the likelihood ratio test when the alternative is Markov of order close to $\log_2 M$. The possibility of using these ideas to test pseudorandom number generators will also be discussed.

AN INFORMATION THEORETIC APPROACH TO DECISION TREE DESIGN,

ROD GOODMAN and PATRICK SMYTH, Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125, USA.

This paper discusses the application of information theoretic measures for the analysis and design of decision trees. We show how the conversion of decision tables into trees can be modelled effectively by appropriate communication channels. This conversion is also shown to be equivalent to deriving optimal prefix codes under certain constraints. Accordingly, we present some bounds on the average depth of a tree designed using our mutual information approach. Techniques to model noise using the channel concept are also presented and the trade-off between noise level, average tree depth, and average mutual information is investigated. This leads to the derivation of a new rule for determining when to terminate a branch during tree design. Uncertain or incomplete data, feature costs, and feature quantization can also be modelled using our channel analogy. In the paper we present our new algorithms together with experimental results based on image classification. Finally, we give an outline of how these models can be extended to the problem of automated rule derivation in expert systems.

SESSION THC2

ALGEBRAIC CODING THEORY II

ON A CLASS OF GENERALIZED GOPPA CODES,

JEAN CONAN and MANSOUR LOELOEIAN, Department of Electrical Engineering, Ecole Polytechnique de Montréal, P.O. Box 6079, Station "A" Montréal, Québec H3C 3A7, Canada.

Based on a Fourier type of transform of n-tuples on a finite field, a class of generalized Goppa codes is proposed which encompasses the entire class of alternate codes. It is shown that our definition of these codes in terms of rational fractions is a unification of recently introduced generalizations of Goppa codes and in fact is equivalent to that of the generalized BCH codes introduced by Chien and Choy for a special case. The spectral decoding procedure of the generalized Goppa codes is carried out with the use of a BCH decoder. It is interesting to mention that the same technique can be applied to the decoding of Goppa codes in the transform domain.

SOME OPTIMAL BINARY CODES WITH DIMENSION 8,

S.M. DODUNEKOV and N.L. MANEV, Bulgarian Academy of Science, P.O. Box 373, Institute of Mathematics, 1090 Sofia, Bulgaria.

Let $n(k,d)$ be the minimum possible length of binary linear code with dimension k and minimum distance d. The exact value of $n(8,d)$ for $d = 32$ and $d = 48$ and more precise bounds for $n(8,d)$, when $d = 34,36,42,44,52,58,60$ are obtained. Also, an update version of the Table 2 given in the authors' paper: Discrete Appl. Math. 12 (1985) 103-114, is presented. At the end improved lower bounds

$$n(k,2^{k-i}) \geq g(k,2^{k-i}) + 3, \text{ for } k \geq 8, \ 3 \leq i \leq k-5$$

$$n(k,2^{k-i}-2) \geq g(k,2^{k-i}-2) + 3, \text{ for } k \geq 9, \ 5 \leq i \leq k-6$$

are proved ($g(k,d) = \sum_{j=0}^{k-1} \lceil d/2^j \rceil$ - Griesmer bound).

OPTIMUM BINARY CYCLIC BURST CORRECTING CODES,

KHALED A.S. ABDEL-GHAFFAR and ROBERT J. McELIECE, Department of Electrical Engineering, California Institute of Technology, Pasadena, CA 91125, USA and ANDREW M. ODLYZKO, AT&T Bell Laboratories, Murray Hill, NJ 07974, USA and HENK C.A. VAN TILBORG, Department of Mathematics and Computer Science, Eindhoven University of Technology, 5600 MB, Eindhoven, The Netherlands.

A code is called a b-burst correcting code if it can correct any single cyclic burst of length b, or less. The length n and redundancy r of a binary b-burst correcting code satisfy $n \leq 2^{r-b+1} - 1$. A binary b-burst correcting code which satisfies this bound with equality is said to be optimum.

In this paper, we prove that for every positive integer b, for every squarefree polynomial $e(x)$ over GF(2) of degree $b-1$ which is not divisible by x, and for every sufficiently large $m \equiv 0 \pmod{m_e}$, where m_e is the least common multiple of the degrees of the irreducible factors of $e(x)$, there exists a primitive polynomial $p(x)$ over GF(2) of degree m such that $e(x)p(x)$ generates an optimum b-burst correcting code of length $2^m - 1$. This implies that for every positive integer b, there exists infinitely many optimum binary cyclic b-burst correcting codes. The basic tools used in the proof are Weil's estimates of character sums with polynomial arguments. We also study in detail optimum binary cyclic codes for $b = 3,4$ and 5. [This research was supported by the Defense Advanced Research Projects Agency, ARPA order 3771, and monitored by the Office of Naval Research under contract number N00014-79-C-0597.]

ELEMENTARY MODULAR REDUNDANCY CODES OF THE REED-SOLOMON TYPE,

W.L. FORSYTHE, CEEC, Box 1299, Ellensburg, WA 98926, USA.

Multiresidue codes with relatively prime submoduli are maximum distance separable, and asymptotically equivalent to Reed-Solomon codes if the submoduli utilize consecutive primes. This embedding of a graded projective Z_M torsion module in a vector space is similar to packing or covering. Applications include long codes, computer architecture and possibly waveform phase modulation using subfrequencies.

SESSION THC3

CODING FOR SPECIAL CHANNELS

CODING FOR 'WRITE-ONCE' MEMORIES WITH MANY UPDATINGS,

GÉRARD D. COHEN, PHILIPPE GODLEWSKI, and MARC BEVERAGGI, CNRS UA 820, ENST, Dept. SYC, 46 rue Barrault, 75013 Paris, France.

Following Rivest and Shamir, we denote by $<v>^t/n$ a womcode allowing t successive writings of one message among v on a n-WOM (write-once memory with n binary positions or wits). We prove:

Proposition. For $r \geq 4$ one can write $t=2^{r-2}+2^{r-4}-1$ times r bits on a (2^r-1)-WOM.

This results is based on the following one on covering radius for codes, which is of independent interest.

Proposition. Hamming codes shortened up to $2^{r-1}+2^{r-2}-1$ times have covering radius at most 4.

We finally give geometrical constructions for $<n>^t/n$ codes with maximal $t=t(n)$. the first values are:

n	=	3	4	5	6	7	8	9	10	11
$t(n)$	=	2	2	3	3	4	4	4	5	≥ 5

TWO CLASSES OF CODES FOR UNEQUAL ERROR PROTECTION,

MAO-CHAO LIN, University of Hawaii, Honolulu, HI 96822, USA, and SHU LIN, Texas A&M University, College Station, TX 77843, USA.

On some occasions, some information symbols in a message are more significant than the other symbols in the same message, and hence require more protection than the other symbols. As a result, it is desired to devise codes with multi-level error-correction capabilities. Another situation where codes with multi-level error-correction capabilities are desired is in broadcast communication systems. An m-user broadcast channel has one input and m outputs. The single input and each output form a component channel. The component channels may have different noise levels, and hence the messages transmitted over the component channels require different levels of protection against errors. In this paper we investigate linear block codes with multi-level error-correction capabilities. These codes are also known as unequal error-protection codes. Two classes of such codes are presented. The first class is given in terms of the parity-check matrices of the codes. This class contains Boyarinov-Katsman codes as a subclass. The second class is a class of cyclic codes of composite length. Each code in this class is a direct-sum of two component codes, and is given in term of its parity polynomial. This class of codes contains Van Gils' codes as a subclass. A decoding algorithm for the first class of codes is devised. This research is supported by NSF Grant ECS 84-18248 and NASA Grant NAG 5-407SA 1.

ON CODING FOR 'STUCK-AT' DEFECTS,

J. MARTIN BORDEN, Worcester Polytechnic Institute, Worcester, MA 01609, USA, and A.J. VINCK, Eindhoven Institute of Technology.

Additive linear codes for use on the defect channel -- a model for computer memories with stuck-at defects -- are studied. Basic properties of both block and convolutional codes are given. Error probabilities are carefully defined and bounded. A reasonably practical convolutional coding scheme is described and simulated. Finally, some codes for a bursty defect channel are described.

AN EFFICIENT CLASS OF UNIDIRECTIONAL ERROR DETECTING/CORRECTING CODES,

DALI TAO, Department of Electrical and Computer Engineering, CARLOS R.P. HARTMANN, School of Computer and Information Science, and P.K. LALA, Department of Electrical and Computer Engineering, Syracuse University, NY 13210, USA.

With the advent of VLSI the difficulty and expense of testing integrated circuit chips have become so great that it is now mandatory to design easily testable chips. As the internal complexity of integrated circuit chips increases, the idea of built-in test becomes more attractive. In general, faults in logic circuits produce either symmetric or asymmetric errors; however, recent research reveals that many VLSI faults produce undirectional errors. So it is important to develop a class of codes to correct certain symmetric errors, while simultaneously detecting all undirectional errors.

We introduce a new class of t-error correcting and all unidirectional error-detecting systematic codes. The codes are constructed by appending $(t + 1)$ blocks of Berger type codes to a linear binary systematic code. These codes are more efficient and less restrictive than codes constructed using other proposed methods. [This work was supported in part by the New York State Center for Advanced Technology in Computer Applications and Software Engineering (CASE Center) at Syracuse University and in part by a grant from the National Science Foundation.]

SESSION THC4

DATA COMPRESSION

A COMPARISON OF DATA COMPRESSION ALGORITHMS,

JANEEN PISCIOTTA, Stevens Institute of Technology, Hoboken, NJ 07030, USA and VICTOR K. WEI, Bell Communications Research, 435 South Street, Morristown, NJ 07960, USA.

We compare several data compression algorithms, including the static Huffman coding, the dynamic Huffman coding, the Lempel-Ziv algorithm, several locally adaptive schemes, and the interval coding scheme. We use Gallager's version of dynamic Huffman coding, and Welch's version of the Lempel-Ziv algorithm. The locally adaptive data compression schemes, which exploit the locality of reference, are due to Bentley, Sleator, Tarjan, and Wei. This class of schemes is based on list updating rules in self-organizing data structures. We use the move-to-front rule and two variants of the transpose rule in our comparison. The interval coding scheme is due to Elias. Large files including English texts, C and FORTRAN source programs, and data are compressed by the various algorithms. The compression ratios are tabulated and compared. The results differ from one category of files to another. Roughly speaking, the Lempel-Ziv algorithm and the move-to-front scheme achieve better compression efficiencies than others.

ADAPTIVE SOURCE MODELS FOR DATA COMPRESSION,

TENKASI V. RAMABADRAN and DAVID L. COHN, Department of Electrical and Computer Engineering, University of Notre Dame, Notre Dame, IN 46556, USA.

Noiseless compression of a finite sequence may be viewed as a two-step process consisting of i) Source modeling and ii) Coding. Efficient coding techniques are now known. The major problem in data compression is, therefore, one of building a source model of a given complexity which assigns the highest probability to the sequence to be compressed. In this presentation, a generalized model called *Conditioned Source Model* is studied. Simple and useful properties of this model are derived using well known Information Theory inequalities. Next the problem of selection of a good set of contexts for this model is addressed and some heuristic approaches are discussed. A technique for reducing the alphabet size of the model which retains the nature of the original alphabet is then introduced. Finally, a new data compression algorithm (called CRAM) is presented. This algorithm uses the alphabet reduction technique, builds the source model adaptively using selective context splitting, and encodes a given sequence by means of arithmetic coding. It is shown to be effective for a variety of computer files.

A NOTE OF THE COMPRESSION FUNCTION OF WORDS OVER ALPHABETS,

M. HASEGAWA, Department of Mathematical Sciences, Lakehead University, Thunder Bay, Ontario P7B 5E1, Canada.

In this study the compression function of words over alphabets is introduced to analyze the structure of words. Consider, for example, a word $p = 1\,1\,0\,1\,0\,1\,0\,1\,1\,1\,1\,0\,1\,0\,1$ $0\,1\,1\,0\,0\,1\,0\,0\,0$ and the following rewriting process: $p \underset{z=110}{\rightarrow} x\,1\,0\,1\,0\,1\,1\,x\,1\,0\,1\,0\,x\,0$ $1\,0\,0\,0 \underset{y=10}{\rightarrow} x\,y\,y\,1\,1\,x\,y\,y\,x\,0\,y\,0\,0 \underset{z=zyy}{\rightarrow} z\,1\,1\,z\,x\,0\,y\,0\,0$, where, in each step, some factor (subword) of p is replaced (substituted) by an "address" symbol. The quadruplet $(x = 1^20, y = 10, z = xy^2, z\ 1^2z \times 0\ y\ 0^2)$ called a representation of p, contains sufficient information to construct the original word p, and presents a view of the structure of p in the following way: $p = ((1^20)(10)^2)1^2((1^20)(10)^2)(1^20)0(10)0^2$. There are many representations of p. Among them, we are interested in representations which give the "shortest length" which will be defined as the value of the compression function of the word p (e.g., $(x = 10,\ y = 1\ x^3,\ z = y\ 1^2,\ z^2\ 0^2\ x\ 0^2)$). This representation expresses p in one of the tightest forms of its structure: $p = (1(10)^31^2)^2\ 0^2(10)0^2$. Some basic properties of this function are studied and, as an application, a characterization of ultimately periodic words by using the compression function is given.

SOURCE MODELING FOR ARITHMETIC CODES WITH APPLICATIONS TO LOW-RATE IMAGE COMPRESSION,

SHARAF E. ELNAHAS and KOU-HU TZOU, GTE Laboratories Incorporated, Waltham, Massachusetts 02254, USA and JAMES G. DUNHAM, Southern Methodist University, Dallas, Texas 75275, USA.

A theory of source modeling for arithmetic coding systems is established based on the concept of source-parsing trees. The arithmetic-coding structure function is defined in terms of source-parsing trees -- namely, conditioning trees. Lower and upper bounds on the performance of arithmetic codes are presented in terms of an average conditional entropy that is obtained through parsing the course by the conditioning tree. For a given tree, the bounds provide a means for the optimal choice of the state-dependent probabilities that are needed for arithmetic codes. The key information-theoretic properties of conditioning trees are discussed along with algorithms for the construction of optimal and suboptimal trees. The theory and algorithms are applied to coding the discrete cosine transform coefficients of digital images. The performance of arithmetic codes is compared to that of a traditional combination of runlength and Huffman codes. The results indicate that binary arithmetic codes outperform runlength codes by a factor of 34% for low-rate coding of the zero-valued coefficients. Hexadecimal arithmetic codes provided a coding rate improvement as high as 28% over truncated Huffman codes for the nonzero coefficients. The complexity of these arithmetic codes is suitable for practical implementation.

SESSION THC5

SEQUENTIAL DECODING

SOME RESULTS IN SEQUENTIAL DECODING,

B.S. KATAKOL and S.L. MASKARA, Department of E and ECE, Indian Institute of Technology, Kharagpur, 721302, India.

In this paper the results of our investigations on different sequential decoding algorithms such as Fano, Minimum distance decoding and Stack have been reported. A modification to the conventional Fano algorithm has been suggested to reduce its computational effort. Employing short constraint length (K) rate 1/2 and rate 1/3 codes with $K = 3$, it has been shown that this modified Fano decoder is computationally efficient. The performance of the modified Fano decoder using rate 1/2 codes with $K = 3$ and $K = 7$ has also been evaluated in AWGN and Rayleigh fading channels. It has been found that the BER performance of the modified Fano decoder is same as the Fano decoder in the BER ranges of practical interest. On the fading channel the modified Fano decoder employing the rate 1/2, $K = 3$ code provides a 2.5 dB SNR advantage as compared to the dual diversity PSK system and a 9.0 dB advantage as compared to a non-diversity PSK system on the same channel. For the purpose of comparing the modified Fano algorithm with other sequential decoding algorithms such as minimum distance algorithm, and Fano algorithm, a minimum distance decoder employing direct mapping only and a microprocessor based Fano decoder, have been implemented. Finally all these algorithms along with Stack and Viterbi algorithms have been compared with respect to the parameters such as storage requirement, computational complexity throughput rate etc.

A BRANCHING PROCESS ANALYSIS OF THE STACK ALGORITHM OVER A BURSTY CHANNEL,

M.J. MONTPETIT, G. DESLAURIERS, and D. HACCOUN, Departments of Electrical Engineering and Applied Mathematics, Ecole Polytechnique, Campus de l'Université de Montréal, Case postale 6079, succursale "A", Montréal, Quebec H3C 3A7 Canada.

A branching process analysis of sequential decoding has yielded interesting results for the average number of computations performed by the stack algorithm over a Gaussian memoryless channel. It is the purpose of this paper to complement these results for a bursty channel. We will use the Gilbert-Eliot channel model and study, with introduction of varying environments in the branching process, the rate b/v, b=1,2, random and semi-random convolutional codes. Results similar to those for the memoryless channel have been obtained for the number of computations. Furthermore, the method gives insight into the behavior of the algorithm in a bursty environment. [This research has been supported in parts by a grant from the National Science and Engineering Research Council of Canada.]

ON SEQUENTIAL DECODING FOR THE GILBERT CHANNEL,

V. SIDORENKO, Institute for Problems of Information Transmission, USSR Academy of Sciences, Ermolovoy 19, Moscow GSP-4, USSR, ROLF JOHANNESSON, Dept. of Computer Eng., University of Lund, P.O. Box 118, S-221 00 Lund, Sweden, and K.SH. ZIGANGIROV, Institute for Problems of Information Transmission.

It is well known that the computational performance of sequential decoding deteriorates drastically when channel errors occur in clusters. Hagenauer (" Sequential decoding for burst-error-channels," NATO Advanced Study Institute on Communication System and Random Process Theory, Darlington, 1977) suggested a feasible modification of sequential decoding which uses a burst-tracking method for better performance. He considers at each step the channel as memoryless but with varying probability of error. In this paper we present a different way of using sequential decoding to exploit the memory of a Gilbert channel. We use a Fano-like metric matched to the channel. Each frame is divided into blocks. The blocks are transmitted after interleaving. The received sequence is deinterleaved in the obvious way. Flags will be used to denote that we are in the bad state. A Fano-like metric m will be calculated for each received symbol according to the following rules:

Situation	State transition	Flag	Metric
No flag & no error:	$G \rightarrow G$	-	$m \leftarrow a_G = \log_2 2(1-P) - R$
No flag & error:	$G \rightarrow B$	Set flag	$m \leftarrow b_G = \log_2 P - R$
If flag & T consecutive error free symbols:	$B \rightarrow G$	Reset flag	$m \leftarrow b_B = \log_2 2Q - R$
Otherwise:	$B \rightarrow G$	-	$m \leftarrow a_B = \log_2(1-Q) - R$

With short interleaving our algorithm seems to be slightly better than Hagenaurer's. [The work was partially supported by the Royal Swedish Academy of Sciences and the Royal Academy of Enginering Sciences in liaison with the Academy of Sciences of USSR and partially by the Swedish Board for Technical Development Grant 85-3303.]

DECODING OF PUNCTURED CONVOLUTIONAL CODES BY THE STACK ALGORITHM,

GUY BÉGIN and DAVID HACCOUN, Department of Electrical Engineering, Ecole Polytechnique de Montréal, Canada.

The punctured convolutional codes are a class of high-rate convolutional codes having the same underlying structure as that of low-rate codes. They have been originally proposed to simplify the Viterbi decoding of high-rate codes. We have successfully applied the stack sequential algorithm to the decoding of punctured codes, taking advantage of their special structure to reduce the complexity of the decoder. Several punctured codes with large memory have been found for different coding rates. Decoding of these codes with refined sequential algorithms have been simulated and show computational improvements of the punctured approach over straightforward decoding. Error performance agrees with bounds obtained from the weight spectra of the codes. An upper bound on the free distance of punctured codes has been formulated. [This research has been supported in part by the National Science and Engineering Research Council of Canada, and by the Fonds FCAR of Québec.]

SESSION THC6

SHANNON THEORY VI

CAPACITY LOSS IN THE HOPFIELD ASSOCIATIVE MEMORY DUE TO QUANTIZATION,

EDWARD C. POSNER, Dept. of Electrical Engineering and Jet Propulsion Laboratory, California Institute of Technology, and EUGENE R. RODEMICH, Jet Propulsion Laboratory, USA.

The Hopfield Associative Memory remembers n-tuples of ± 1's by changing the state of a probe vector until the probe is stable. Changes are caused by each component adjusting itself to the signum of a linear sum of all the other components via a connection matrix T_{ij}. When T_{ij} is the sum of the outer products of the m memories to be stored, it is known that the asymptotic capacity (i.e., value of m with random independent memories such that the stable point reached is correct, provided that the initial probe is more than half right) is $n/(2\log n)$. This paper studies the loss in capacity if we quantize the sums of outer products T_{ij} before taking the sum. It is shown that the capacity loss factor is the same as the loss of channel capacity in the additive white Gaussian channel when we quantize the channel output. For instance, if we hard-limit the output, the capacity drops by the familiar factor of $2/\pi$ or $2.0dB$. For memory implementation, three-level quantization of the outer-product connection matrix is quite feasible; the loss in memory capacity (if the optimum thresholds are chosen) is only 195, and 46% of the T_{ij} are zero. The proof that the channel capacity loss and memory capacity loss factors are the same is not hard, given the proof of the original $n/(2\log n)$ capacity result for the Hopfield Associative Memory with sum of outer products connection matrix, which will appear in 1987 in the IT Transactions.

INFORMATION CAPACITY OF MODIFIED ASSOCIATIVE MEMORY MODELS,

ANTHONY KUH and BRADLEY W. DICKINSON, Dept. of Electrical Engineering and Computer Science, Princeton University, Princeton, NJ 08544, USA.

Associative memory networks, consisting of highly interconnected binary valued cells, have been used to model neural networks. Asymptotic bounds have been found for the information capacity of these networks. We first derive the asymptotic information capacity of these networks using results from normal approximation theory and theorems about exchangeable random variables. Then we present some more general models that retain much of the simple structure of the original networks. Many of the standard associative networks use a decision rule involving a thresholding of a linear sum of weighted cell values. We consider networks where the thresholding operation is replaced by a random operation. A second modification deals with networks where cell interconnectivity may vary. We present solutions for the capacity of these modified associative memories.

THE EMPIRIC ENTROPY, A NEW APPROACH TO NONPARAMETRIC ENTROPY ESTIMATION,

EDWARD J. DUDEWICZ, Department of Mathematics, Syracuse University, Syracuse, NY 13210, USA and EDWARD C. VAN DER MEULEN, Department of Mathematics, Katholieke Universiteit Leuven, Celestijnenlaan 200 B, B-3030 Leuven, Belgium.

Since Shannon's pioneering work (1948), the topic of entropy maximization has been of great theoretical and applied interest. Entropy principles play a key role in recent applications, such as spectral analysis, speech coding, and pattern recognition. The entropy $H(f) = -\int f(x) log f(x) dx$ of a continuous probability density $f(x)$ usually needs to be estimated nonparametrically from a random sample $X_1, \ldots, X_n$, since commonly $f(\cdot)$ is unknown. In this contribution we briefly review previous work on estimation of $H(f)$ and then provide a class of new entropy estimators called empiric entropies via an entropy-like functional of the empiric density function and generalizations thereof. The relationships and differences with previous entropy estimators are pointed out, and several interesting properties of the new estimator are shown.

ON THE DETERMINISTIC AND RANDOM CODING CAPACITIES OF DISCRETE ARBITRARILY VARYING CHANNELS WITH CONSTRAINED STATES

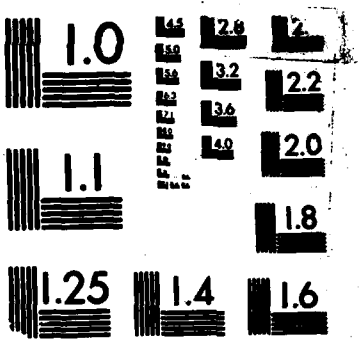
IMRE CSISZAR, The Mathematical Institute of the Hungarian Academy of Sciences, Realtanoda u. 13-15, H-1053 Budapest, Hungary, and PRAKASH NARAYAN, Electrical Engineering Department, University of Maryland, College Park, MD 20742, USA.

We consider the deterministic coding capacities of the following discrete arbitrarily varying channel (AVC) models with constraints on the channel states: (a) the binary adder channel, (ii) the arithmetic adder channel, and (iii) the multiplier channel. For cases (i) and (ii), the deterministic coding capacities equal the respective random coding capacities. For the multiplier channel in case (iii) the deterministic coding capacity, under suitable conditions, is shown to lie *strictly* between zero and the random coding capacity. The issue of random coding capacities of general discrete AVCs with codeword and state constraints is also addressed.

AUTHOR INDEX

AD-A193 252 IEEE INTERNATIONAL SYMPOSIUM ON INFORMATION THEORY (ISIT): ABSTRACTS OF P.. (U) MICHIGAN UNIV ANN ARBOR ROBINSON OCT 86 AFOSR-TR-88-0287 AFOSR-87-0046 3/3

UNCLASSIFIED F/G 12/9 NL



MICROCOPY RESOLUTION TEST CHART

END

DATE

FILMED

DTIC

JULY 88