Lecture Notes in Computer Science 1133
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Jean-Yves Chouinard Paul Fortier
T. Aaron Gulliver (Eds.)

Information Theory and Applications II

4th Canadian Workshop
Lac Delage, Québec, Canada, May 28-30, 1995
Selected Papers

Springer

Volume Editors

Jean-Yves Chouinard
Department of Electrical Engineering, University of Ottawa
161 Louis-Pasteur, Ottawa, Canada, K1N 6N5
E-mail: chouinar@elg.uottawa.ca

Paul Fortier
Département de génie électrique et de génie informatique, Université Laval
Cité Universitaire, Québec, Canada, G1K 7P4
E-mail: fortier@gel.ulaval.ca

T. Aaron Gulliver
Department of Electrical and Electronic Engineering
University of Canterbury
Private Bag 4800, Christchurch, New Zealand
E-mail: gulliver@elec.canterbury.ac.nz

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information theory and applications : ... Canadian workshop ; proceedings. - Berlin ; Heidelberg ; New York ; London ; Paris ; Tokyo ; Hong Kong ; Barcelona ; Budapest : Springer

4. Lac Delage, Québec, Canada, May 1995 : selected papers.
(Lecture notes in computer science ; 1133)
ISBN 3-540-61748-5
NE: GT

CR Subject Classification (1991): E.4, E.3,F.2, I.4, I.5, I.6, G.2, G.3, B.4

ISSN 0302-9743
ISBN 3-540-61748-5 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10513584 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

The 1995 Canadian Workshop on Information Theory was held in Lac Delage, Québec from May 28 to May 31. This was the fourth workshop to be held under the auspices of the Canadian Society of Information Theory. The previous three workshops took place in Saint-Jovite, Québec in 1987, Sidney, British Columbia in 1989, and Rockland, Ontario in 1993. The purpose of the workshops has been to provide an informal setting for Canadian researchers to meet and exchange ideas on information theory. We were pleased to welcome a number of participants from the United States and France among the 44 attendees, as was the case in 1993. There were 30 regular presentations given at the workshop as well as presentations by three invited speakers.

This volume is the second proceedings to be published from the Canadian Workshop on Information Theory. Following the workshop, participants were asked to submit a manuscript and each paper has been subject to peer review. An extensive list of reviewers appears at the end of the preface. This volume contains 21 papers written by the workshop speakers and co-authors, including the papers from the invited speakers. The papers are grouped into five sections: algebraic coding, cryptography and secure communications, decoding methods and techniques, coding and modulation for fading channels, and signal processing and pattern recognition. A brief summary of the papers in each section is given below.

Algebraic Coding

This section begins with the paper by the invited lecturer, Professor Gérald E. Séguin. This paper presents a study of the algebraic structure of linear codes invariant under a given permutation. Séguin derives expressions for determining the number of such codes as well as methods to decompose them into component codes. In the next paper, Pedersen and Polemi propose a novel method to construct longer codes by combining algebraic geometric Goppa codes. They discuss the minimum distance properties of these new codes. Gulliver and Bhargava present the construction of multiple circulant quasi-cyclic codes over $GF(5)$. In terms of distance properties, they show that several codes are optimal whereas the others provide a lower bound on the maximum possible minimum distance.

Cryptography and Secure Communications

Youssef and Tavares introduce static and dynamic information leakage measures between the inputs and outputs of randomly selected Boolean functions as cryptographic criteria. In particular, they demonstrate that the expected values of information leakages decrease significantly with the number of input variables. Aakvaag, Lacaze and Duverdier investigate a scrambling method to ensure message privacy. By introducing controlled periodic clock changes into transmitted analog signals, the interception of messages can be prevented while the exact knowledge of the corresponding reconstruction filter allows their reconstitution.

Assuming wide sense stationary sources of information, they derive the conditions under which perfect reconstruction can be achieved. In a companion paper, Duverdier, Lacaze and Aakvaag study the application of linear time-varying periodic filtering of stationary processes for message scrambling and introduce a reconstruction method based on their cyclostationary properties. In particular, they show that this method results in an unconventional form of spread spectrum which facilitates the reconstruction of an analog signal and, in the case of a binary signal, can correct errors caused by frequency selective fading.

Decoding Methods and Techniques

The first paper of this section is written by the invited lecturer, Professor Gérard Battail. Professor Battail presents a comprehensive survey of random codes with an emphasis on pseudo-random systematic convolutional codes. He discusses the properties of strongly random-like and weakly random-like codes and shows that by combining several random-like codes (some of which are random with small minimum distance), it is possible to control the tail distribution of the codes and hence increase the channel reliability. Guinand, Lodge and Papke propose two new interleaving methods, one based on number theory and the other on finite projective planes, for iterative maximum a posteriori (MAP) decoding of product block codes. They show that, by using large interleavers, it is possible to eliminate certain problematic error patterns and hence obtain an improved error rate performance. Gravel, Drolet and Rozon present a reduced complexity VLSI decoder design for concatenated codes consisting of an irreducible cyclic inner code and a Reed-Solomon outer code. Using the Berlekamp-Massey algorithms in the time and frequency domains, this concatenation leads to a significant reduction in the hardware complexity of the decoder. Lee and Kschischang present a method, based on atomic span modification, to construct a general class of non-minimal trellises for linear block codes having a regular structure. In this case, the code trellis can be split into a number of structurally identical parallel subtrellises. The authors propose a multiprocessor implementation that uses coset decoding for soft-decision decoding with a parallel trellis search. Esmaeili, Gulliver and Secord explore the trellis complexity and state connectivity of linear codes using trellis oriented generator matrices and atomic codewords. A simple yet comprehensive complexity analysis is given for the minimal L-section trellis diagram of Reed-Muller codes. Jürgensen and Konstantinidis give a mathematical description of discrete channels in which the transmitted symbols are affected by substitution, insertion and deletion errors. The decidability of unique decoding for error correction codes is investigated for non-probabilistic channels.

Coding and Modulation for Fading Channels

This section begins with the paper of Boudreau and Viens who investigate the performance of a reduced complexity linear predictive receiver for 4-ary continuous phase modulation (CPM) signals in Rayleigh flat-fading channels. Using

a maximum likelihood sequence estimator (MLSE) with the q-ary soft-output Viterbi algorithm (QSOVA), promising results, in terms of bit error rate and receiver complexity, are obtained for power-limited channels such as mobile satellite channels. In the following paper, Nassar and Soleymani introduce a novel receiver design with a parallel structure for the detection of differentially encoded M-ary phase shift keying (MPSK) symbols in rapidly changing phase environments. The authors demonstrate that this receiver, which approximates maximum likelihood symbol estimation, outperforms DPSK as well as multiple symbol differential detection (MSDD) with an increase in receiver complexity of less than an order of magnitude. D'Amours and Yongaçoğlu study the spectral efficiency of a hybrid code division multiple access system using both direct sequence and frequency hopping schemes (DS/FH-CDMA) that employ M-ary frequency shift keying (MFSK) modulation. Comparison between non-coherent MFSK, combined MFSK and DPSK and wideband multitone FSK (MT-FSK) in Rayleigh fading channels indicates that MFSK with rate 1/2 dual-k coding provides the best spectral efficiency performance.

Signal Processing and Pattern Recognition

This section begins also with the paper of an invited lecturer, Professor H. Vincent Poor. Professor Poor presents an interesting overview of the recent developments of wavelet signal decomposition and reconstruction from a multiresolution signal analysis perspective. He describes cyclic wavelet transforms defined over finite fields and gives an application of multiresolution analysis to the design of multilevel error control coding. In the following paper, Mandal, Panchanathan and Aboulnasr study wavelet searching methods with reduced computational complexity for image source coding applications. The authors also suggest a reduced complexity adaptive algorithm for wavelet packet decomposition which provides good coding performance. Volden, Giraudon and Berthod use information theory to introduce new measures of image redundancy based on the entropy of Markov random fields. They present comparative results between these redundancy measures and the classical correlation coefficient measure for the case of satellite images. Gauvin, Doucet, Gingras and Chevrette present an algorithm for automatic target recognition which makes use of a template matching technique based on distance classifier correlation filters (DCCF). They investigate the object classes discrimination performance as a function of the training set. To improve the functionality of prosthetic devices, Gallant, Morin and Peppard present a new method for the extraction of myoelectric signals and their classification into distinct muscle contraction classes. The approach adopted by the authors, which involves a neural network-based classifier, results in a high correct classification rate for these signals. Liao and Pawlak propose a variant of the method of moments for Chinese character recognition. Using the Legendre moment feature space instead of the Central moment feature space, the authors show that significant improvement in character recognizing ability can be achieved.

Acknowledgements

We would like to express our warm thanks to the following reviewers for generously donating their valuable time. Without their assistance, this volume would not have been possible.

Behnaam Aazang
Tyseer Aboulnasr
Yaser S. Abu-Mostafa
Jakob D. Anderson
Jean Belzile
Sergei V. Bezzateev
Gerald Bolding
Daniel Boudreau
Joseph Boutros
Gilles Brassard
Richard Buz
Lorne Campbell
Jean Conan
Vladimir Cuperman
Claude D'Amours
F. Daneshgaran
Christophe Deutsch
Germain Drolet
Morteza Esmaeili
E. Barry Felstead
Hendrik C. Ferreira
Terrence L. Fine
François Gagnon
Peter J. Gallant
Christian Gehrmann
Allen Gersho
Denis Gingras
Dominic Grenier
Roshdy H.M. Hafez
Joachim Hagenauer
Anwar Hasan
A. S. J. Helberg
Paul Ho
Hideki Imai
Helmut Jürgensen
Tsutomu Kawabata
Hiroshi Kondo
Evangelos Kranakis
Adam Krzyżak
Frank R. Kschischang
Michel Lecours
Shu Lin
Alan Lindsey
John H. Lodge
Lloyd J. Mason
E. Masry
Robert J. McEliece
Laurence B. Milstein
Michael Moher
Lim Nguyen
Haluk Öğmen
Paul C. Van Oorschot
Erik Paaske
Jens Peter Pedersen
S. Eli Posner
Gregory J. Pottie
Sven Riedel
Jean-François Rivest
Ron M. Roth
Leslie A. Rusch
Michael Sablatash
Gérald Séguin
Asrar U. Sheikh
Blanca R. M. Sosa
Elvino Sousa
R. Michael Tanner
Stafford E. Tavares
Desmond P. Taylor
Chokri Trabelsi
Ari Trachtenberg
Marc Tremblay
Victor Keh-Wei Wei
Stephen B. Wicker
Mladen Victor Wickerhauser
Tet Yeap
Abbas Yongaçoğlu
André Zaccarin
Denis Zaccarin

The editors are also grateful to the following organizations for their support of the workshop:

- Canadian Society of Information Theory
- Carleton University
- IEEE Information Theory Society
- IEEE Region 7
- Laval University
- University of Ottawa

June 1996

Jean-Yves Chouinard
Paul Fortier
T. Aaron Gulliver

Table of Contents

Coding and Modulation for Fading Channels

Signal Processing and Pattern Recognition