G. Cohen S. Litsyn
A. Lobstein G. Zémor (Eds.)

Algebraic Coding

First French-Israeli Workshop
Paris, France, July 19-21, 1993
Proceedings

Springer-Verlag
Berlin Heidelberg New York
London Paris Tokyo
Hong Kong Barcelona
Budapest

Lecture Notes in Computer Science 781
Edited by G. Goos and J. Hartmanis

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

Volume Editors

Gérard Cohen
Antoine Lobstein
Gilles Zémor
École Nationale Supérieure des Télécommunications
46 rue Barrault, F-75634 Paris Cedex, France

Simon Litsyn
Department of Electrical Engineering, Tel Aviv University
Ramat Aviv 69978, Israel

CR Subject Classification (1991): E.3-4, G.2

ISBN 3-540-57843-9 Springer-Verlag Berlin Heidelberg New York
ISBN 0-387-57843-9 Springer-Verlag New York Berlin Heidelberg

CIP data applied for

Typesetting: Camera-ready by author
SPIN: 10131992 45/3140-543210 - Printed on acid-free paper

PREFACE

The first French-Israeli Workshop on Algebraic Coding took place at Ecole Nationale Supérieure des Télécommunications, Paris, July 19-21, 1993. It was a continuation of a French-Soviet Workshop hold in 1991 and edited by the same board (Springer-Verlag LNCS 573).

Convolutional codes and special channels

V. Balakirsky formulates a necessary and sufficient condition for a linear convolutional time-variant encoder to be noncatastrophic.
G. Kaplan, S. Shamai and Y. Kofman address code design and selection rules under power and decoding delay constraints for a slowly-fading channel modeling a mobile communication system.
G. Poltyrev and J. Snyders consider the assignment of codes to users of a multiple access channel, allowing correction of errors and separation of messages, under the hypothesis that the subset of active users is known to the receiver.
V. Blinovsky and M. Pinsker obtain an upper bound on the number of codewords which must be stored in order to achieve capacity when applying list decoding to an arbitrarily varying channel.

Covering codes

I. Honkala studies the problem of lowerbounding the minimum cardinality of a code with given length n and covering radius 1, in the case when the code is binary and n is congruent to 5 (mod 6).
E. Kolev and I. Landgev address the same problem for mixed binary/ternary codes with length up to 8 and covering radius up to 3.
A. Lobstein and V. Pless present a new table for the smallest length of a binary linear code with given codimension m and covering radius r, for $m \leq 24$ and $r \leq 12$.
I. Bocharova and B. Kudryashov give a new upper bound for the covering radius of convolutional codes, by means of random coding.

Cryptography

O. Delos and J.J. Quisquater describe a multi-signature scheme involving cooperating entities, with no interaction needed between the cosigners.
D. Naccache and D. M'Raïhi present an efficient alternative approach to Montgomery's algorithm for modular operations.
C. Blundo, A. De Santis, L. Gargano and U. Vaccaro consider the problem of designing efficient secret sharing schemes with veto capabilities from qualified minorities.
J.P. Tillich and G. Zémor study weaknesses and strengths of group-theoretic hash functions based on computations in arithmetic groups $SL_2(\mathbf{F}_p)$.

Sequences

S. Bitan and T. Etzion present new constructions for optimal optical orthogonal codes, i.e. families of w-sets of integers modulo n in which no difference is repeated.
A. Gavish and A. Lempel consider so-called complementary pairs of sequences over the alphabet $\{-1, 0, 1\}$. A pair of words is complementary if for a given nonzero shift their aperiodic autocorrelation functions sum up to zero. The authors are interested in minimizing the number of zeros in complementary pairs: they derive some tight bounds on this quantity.
R. Roth considers sequences having rth order spectral null at zero frequency. Upper bounds are derived for the size of the set of all such sequences. Some subsets defined as null spaces of certain submatrices of Hadamard matrices provide codes with codewords belonging to the considered set and large minimal distance.
A. Barg uses the cyclic structure of shortened Kerdock codes to present a family of codes with asymptotically optimal correlation properties.

Graphs and codes

N. Alon and B. Sudakov solve a problem due to Ahlswede *et al.* concerning the maximal number of subsets of constant-weight binary words, such that in each pair of subsets it is possible to find a pair of nonintersecting words, one from each. It turns out that asymptotically, the maximal number of subsets is equal to half of the total number of constant-weight words.
O. Moreno and V. Zinoviev give sufficient conditions for 4-regular graphs to have 3-regular subgraphs by variations on the use of the Chevalley-Warning theorem.
M. Karpovsky, S. Chaudhry, L. Levitin and C. Moraga present bounds and constructions for codes detecting and correcting given error patterns caused by faulty processing elements in multiprocessor systems.

Sphere packings and lattices

A. Bonnecaze and P. Solé construct formally self-dual binary codes and unimodular lattices using quaternary codes. They obtain new constructions of Leech and Gosset lattices.
P. Boyvalenkov and S. Nikova propose a new method for obtaining lower bounds on the size of a spherical t-design, with special emphasis on the cases $t = 9$ or 10.
G. Poltyrev constructs a class of lattices from linear codes using Conway-Sloane construction A, and shows that they achieve capacity for the unrestricted AWGN channel.
P. Loyer and P. Solé generalize the Conway-Sloane lattice decoding algorithm to the L_p norm, computing, in particular, some Voronoi diagrams and covering radii.
O. Amrani, Y. Be'ery and A. Vardy develop new fast algorithms for the soft decoding of the Golay code and the Leech lattice.

Bounds for codes

S. Kovalov derives new conditions that the last element of the distance spectrum of optimal binary codes should satisfy.
S. Litsyn and A. Vardy prove that the code with parameters $(10, 40, 4)$ is unique. This allows them to derive new upper bounds on the number of words in single-error-correcting codes of lengths 10 and 11, namely 78 and 156, respectively.
G. Kabatianski and A. Lobstein provide a new upper bound for binary arithmetic codes, which is asymptotically better than previously known bounds.
G. Cohen, L. Huguet and G. Zémor derive new bounds on the maximum possible dimension of binary codes in terms of their generalized distances.
G. Zémor introduces threshold probabilities θ of linear codes when studying residual error probability; in particular, the residual error probability is shown to always be an exponential function of the minimal distance when the channel error probability is separated from θ.
J. Rifa-Coma gives a decoding algorithm for BCH codes that achieves a little more than the conventional algorithms in the case when the designed and true minimum distances differ.
N. Sendrier analyses the trade-off for error-correcting codes between algorithmic complexity and decoding performance. Low-rate product codes in particular, although of poor minimum distance, possess an efficient natural decoding algorithm.
I. Dumer and P. Farrell study the performance of linear codes on the erasure channel; in particular the case of BCH and concatenated codes is considered.

This meeting was sponsored by the Centre National de la Recherche Scientifique, l'Association Franco-Israelienne de Recherche Scientifique et Technique, le Ministère de l'Enseignement Supérieur et de la Recherche, the French Section of IEEE, and ENST.

We would like to thank the referees,
N. Alon, B. Arazi, A. Barg, G. Battail, R. Calderbank, G. Cohen, J.L. Dornstetter, I. Dumer, S. Eliahou, T. Etzion, M. Girault, I. Honkala, G. Kabatianski, S. Kovalov, J. Lahtonen, A. Lempel, S. Litsyn, A. Lobstein, O. Moreno, V. Pless, G. Poltyrev, S. Qiu, J.J. Quisquater, J. Rifa-Coma, N. Sloane, P. Solé, H. van Tilborg, R. Zamir, G. Zémor.

December 1993 G. Cohen, S. Litsyn, A. Lobstein, G. Zémor

AFTERMATH

As mentioned in the foreword, the French-Soviet workshop took place in july 1991 ; one month later, the USSR collapsed. A few months after the French-Israeli meeting, Jericho and Gaza underwent a dramatic change of status. Understandably, we have become increasingly concerned as to the consequences of the choice of our partner for the next binational event. Indeed, so much so that we decided to switch to a politically invariant characterization of our workshop. We are now preparing the *first Mediterranean Workshop on Algebraic Coding*: this decision was reached only after careful study, and has been approved by earthquake forecast experts.


ECOLE NATIONALE SUP
FORCES ELEMENTAIRES POUR LES
TRANSMISSIONS

CONTENTS

Graphs and codes

Sphere packings and lattices

Bounds for codes