

NORTH-HOLLAND
MATHEMATICAL LIBRARY

Covering Codes

G. COHEN
I. HONKALA
S. LITSYN
A. LOBSTEIN

North-Holland

Covering Codes

Gérard COHEN

ENST, Paris, France

Iiro HONKALA

University of Turku, Finland

Simon LITSYN

Tel-Aviv University, Israel

Antoine LOBSTEIN

CNRS - ENST, Paris, France



1997

ELSEVIER

Amsterdam – Lausanne – New York – Oxford – Shannon – Tokyo

ELSEVIER SCIENCE B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

ISBN: 0 444 82511 8

© 1997 Elsevier Science B.V. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher, Elsevier Science B.V., Copyright & Permissions Department, P.O. Box 521, 1000 AM Amsterdam, The Netherlands.

Special regulations for readers in the U.S.A. – This publication has been registered with the Copyright Clearance Center Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923. Information can be obtained from the CCC about conditions under which photocopies of parts of this publication may be made in the U.S.A. All other copyright questions, including photocopying outside of the U.S.A., should be referred to the publisher.

No responsibility is assumed by the publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein.

This book is printed on acid-free paper

Printed in The Netherlands

COVERING CODES

North-Holland Mathematical Library

Board of Honorary Editors:

M. Artin, H. Bass, J. Eells, W. Feit, P.J. Freyd, F.W. Gehring,
H. Halberstam, L.V. Hörmander, J.H.B. Kemperman, H.A. Lauwerier,
W.A.J. Luxemburg, F.P. Peterson, I.M. Singer and A.C. Zaanen

Board of Advisory Editors:

A. Björner, R.H. Dijkgraaf, A. Dimca, A.S. Dow, J.J. Duistermaat,
E. Looijenga, J.P. May, I. Moerdijk, S.M. Mori, J.P. Palis, A. Schrijver,
J. Sjöstrand, J.H.M. Steenbrink, F. Takens and J. van Mill

VOLUME 54



ELSEVIER

Amsterdam – Lausanne – New York – Oxford – Shannon – Tokyo

To

Aude, Clairette and Maurice

Aino, Kauko and Juha

Maya, Elena, Lola and Nathan

Martine, Doud and André

Preface

Covering and packing the euclidean space by spheres are old and well-known problems. The discrete counterpart of the packing problem has been extensively studied within the theory of error-correcting codes. Its dual, the covering problem, has received much less attention over the years. The last decade, however, has witnessed the blossoming of active research in the area, now materialized in the publication of over 500 papers. We feel that during these ten years the area of covering codes has come of age and developed into an elegant discipline with its own flavour and techniques. Our purpose is, on the one hand, to give an account on the state of the art in the theory of covering codes and, on the other hand, to show how a number of issues are related to – or can be viewed as – covering problems.

In a basic covering problem, we have a vector space over a finite alphabet which we wish to cover with as few spheres of a given radius as possible. This means that we can approximate any point in the space by one or more of the centres with a given accuracy. The covering problems are mathematically and aesthetically appealing in their own right, and lend themselves to technical applications, e.g., data compression.

This book is intended for people involved in communication, algorithms, computer science, discrete mathematics, geometry, algebra or number theory. We have strived to remain accessible to a wide audience, although a minimal background in coding theory, algebra and discrete mathematics is occasionally required. The chapters are fairly independent, which should allow nonlinear reading.

Roughly speaking, the first half of the book is about the covering radius of codes – and we shall emphasize binary codes – whereas the second half deals with generalizations and related problems. We begin with basic definitions and results in the first two chapters. Chapters 3, 4 and 5 are devoted to constructing codes with small covering radius. In Chapter 4 we study normality, the amalgamated direct sum construction and various generalizations. Chapter 5 focuses on linear codes. In Chapters 6 and 7, we present nonexistence results for nonlinear and linear codes, and show how to improve on

the sphere-covering bound. In Chapter 8 bounds are derived on the maximum possible covering radius of a code with a given length, cardinality and minimum or dual distance. In the next two chapters we study the covering radius of certain families of codes including the Reed-Muller and BCH codes. In Chapter 11 we give a thorough account of perfect codes. Chapter 12 is devoted to asymptotical covering radius problems. The next two chapters discuss natural generalizations of the covering radius problem, like weighted coverings, multiple coverings and multiple coverings of deep holes. Chapter 15 deals with a more recreational application, namely, how to use covering codes in connection with football pools. Chapter 16 studies partitions of the binary space into tiles, i.e., cosets of a given set. In the next chapter, we study a general model of constrained memories; it turns out to rely on the worst-case behaviour of the covering radius of shortened codes. In Chapter 18 we explore the connections between graphs, groups and codes and how specific techniques pertaining to these three areas are intertwined. Chapter 19 is devoted to variations on the theme of perfect coverings by spheres, namely coverings by unions of shells, by spheres of two or more radii, or by spheres all of different radii. In Chapter 20 we study various complexity issues related to the field.

We are greatly indebted to Noga Alon, Volodya Blinovskii, Sasha Davydov, Tuvi Etzion, Peter Frankl, Philippe Godlewski, Laurent Habsieger, Heikki Härmäläinen, Juha Honkala, Olivier Hudry, Osnat Keren, Ilia Krasikov, Tero Laihonon, Françoise Levy-dit-Vehel, Skip Mattson, Patric Östergård, Arto Salomaa, Juriaan Simonis, Jakov Snyders, Patrick Solé, Aimo Tietäväinen, Alex Vardy, Gilles Zémor and Victor Zinoviev for their comments and inspiring discussions.

We gratefully acknowledge the assistance of Gloria Garcia, Titia Kraaij, Manuel Moreni, Michelle Nahum and Arjen Sevenster.

List of Symbols

- \mathbb{N} set of nonnegative integers
- \mathbb{Z} set of integers
- \mathbb{Q} set of rational numbers
- \mathbb{R} set of real numbers
- \mathbb{C} set of complex numbers
- \mathcal{S}_n symmetric group on $\{1, 2, \dots, n\}$
- $:=$ is equal to, by definition
- $\lfloor x \rfloor$ floor function, the largest integer less than or equal to x
- $\lceil x \rceil$ ceiling function, the smallest integer greater than or equal to x
- $[i, j]$ $\{\ell \in \mathbb{Z} : i \leq \ell \leq j\}$
- $A \subseteq B$ set A is included in set B
- $A \subset B$ set A is included in set B and A cannot be equal to B
- δ_{ij} Kronecker symbol
- $\binom{a}{b}$ binomial coefficient
- $\mathbb{Z}_q = \{0, 1, \dots, q-1\}$ additive group of integers modulo q
- $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}; \mathbb{F}_q$ finite fields
- \mathbb{F}_q^* the multiplicative group of \mathbb{F}_q
- $\psi_u(\mathbf{x})$ additive character of \mathbb{F}_q
- \mathcal{Q} arbitrary alphabet of size q

$\mathbf{a} = (a_1, a_2, \dots, a_n) = (a_1 a_2 \dots a_n) = a_1 a_2 \dots a_n$, $\mathbf{b}_i = b_{i,1} \dots b_{i,n}$, \mathbf{c}, \dots vectors (usually $(0, 1)$ -vectors), generally assumed to be row vectors

\mathbf{a}^\pm the $(-1, 1)$ -vector obtained from a binary $(0, 1)$ -vector \mathbf{a} by changing 0's to 1's and 1's to -1 's

$\bar{\mathbf{a}}$ the complement of \mathbf{a} , i.e., the vector obtained from \mathbf{a} by changing 0's to 1's and 1's to 0's

$\mathbf{A} = (a_{i,j})$, \mathbf{B} , \mathbf{C}, \dots matrices

\mathbf{A}^T the transpose of matrix \mathbf{A}

$\mathbf{1}$, $\mathbf{0}$ all-1 or all-0 row, column or matrix (of size determined by the context)

$\mathbf{1}^n$, $\mathbf{0}^n$ all-1 or all-0 vector of length n

$\mathbf{1}^{n \times m}$, $\mathbf{0}^{n \times m}$ all-1 or all-0 matrix of size $n \times m$

\mathbf{I} identity matrix

\mathbf{I}_n identity matrix of size $n \times n$

$(\mathbf{x}|\mathbf{y})$ or (\mathbf{x}, \mathbf{y}) concatenation of \mathbf{x} and \mathbf{y}

$\langle \mathbf{x}, \mathbf{y} \rangle$ scalar product of \mathbf{x} and \mathbf{y}

$\mathbf{x} * \mathbf{y}$ componentwise product of \mathbf{x} and \mathbf{y}

$\text{supp}(\mathbf{x})$ support of \mathbf{x}

$w(\mathbf{x})$ Hamming weight of \mathbf{x}

\mathbf{e}_i binary vector with support equal to $\{i\}$

$\pi(\mathbf{x})$ parity check of \mathbf{x}

$d(\mathbf{x}, \mathbf{y})$ Hamming distance between \mathbf{x} and \mathbf{y}

$B_i(\mathbf{x})$ Hamming sphere (or ball) of radius i centred at \mathbf{x} ; $B_i^n(\mathbf{x})$ may be used when it is important to have n specified

$B_i(X) = \cup_{\mathbf{x} \in X} B_i(\mathbf{x})$

$V_q(n, i)$ size of the Hamming sphere of radius i ; subscript q may be dropped in the binary case

$S_i(\mathbf{x})$ set of vectors at distance i from \mathbf{x}

S_i set of vectors of weight i

\mathbb{E}^n set of binary even weight vectors of length n

$\mathcal{A}_i = \mathcal{A}_i(C)$ number of words of weight i in code C

$\mathcal{A}_i(\mathbf{x})$ $|\{\mathbf{c} \in C : d(\mathbf{c}, \mathbf{x}) = i\}|$

$\mathcal{B}_i = \mathcal{B}_i(C)$ distance distribution of C

$C_a^{(i)}$ subcode $\{\mathbf{c} \in C : c_i = a\}$

$\langle A \rangle$ vector space generated by A

$k = k(C) = \dim(C)$ dimension of a linear code C

$R = R(C)$ covering radius of C

$d = d(C)$ minimum distance of C

$d^\perp = d^\perp(C)$ minimum distance of C^\perp , the dual code of a linear code C

$e = e(C) = \lfloor (d(C) - 1)/2 \rfloor$ error-correcting capability of C

$\mu(C)$ density of C

$\mathbf{G} = \mathbf{G}(C)$ generator matrix of a linear code C

$\mathbf{H} = \mathbf{H}(C)$ parity check matrix of a linear code C

$\kappa = \kappa(C) = \log_2 |C|/n = k(C)/n$ information rate of C

$\delta = \delta(C) = d(C)/n$ normalized distance of C

$\delta^\perp = \delta^\perp(C) = d^\perp(C)/n$ normalized dual distance of C

$\rho = \rho(C) = R(C)/n$ normalized covering radius of C

$[n, k, d]R$ binary linear code of length n , dimension k , minimum distance d , covering radius R ; d or R may be dropped when irrelevant

$(n, K, d)R$ binary (not necessarily linear) code of length n , cardinality K , minimum distance d , covering radius R ; d or R may be dropped when irrelevant

$t[n, k]$ smallest covering radius among all $[n, k]$ codes

$t(n, K)$ smallest covering radius among all (n, K) codes

$k[n, R]$ smallest dimension of a binary linear code with length n and covering radius R

$K(n, R)$ smallest cardinality of a binary code with length n and covering radius R

$\ell(m, R)$ smallest length of a binary linear code of covering radius R and codimension (or redundancy) m

$a[n, d]$ maximal dimension of a binary linear code of length n and minimum distance d

$A(n, d)$ maximal cardinality of a binary code of length n and minimum distance d

$n[k, d]$ smallest length of a binary linear code of dimension k and minimum distance d

$g[k, d]$ Griesmer bound on $n[k, d]$

$[n, k, d]_q R, (n, K, d)_q R, t_q[n, k], t_q(n, K), k_q[n, R], K_q(n, R), \ell_q(m, R), a_q[n, d], A_q(n, d), n_q[k, d]$ and $g_q[k, d]$ are the corresponding notations for the q -ary case

$F(v, k)$ minimal cardinality of a $2-(v, k, 1)$ covering design

C° code C shortened in one coordinate

C^* code C punctured in one coordinate

\widehat{C} code C extended

$A \oplus B$ direct sum of codes A and B

$A \dot{\oplus} B$ amalgamated direct sum of A and B

$BCH(e, m)$ primitive BCH code of length $2^m - 1$ and designed distance $2e + 1$

$BCH_h(e, m)$ nonprimitive BCH code of length $(2^m - 1)/h$ and designed distance $2e + 1$

$GOP(L, g)$ Goppa code with defining set L and polynomial g

HAD_n Hadamard code of length n

\mathcal{H}_m Hamming code of length $2^m - 1$

\mathcal{P}_m Preparata code of length 2^m , m even

$QR(p)$ quadratic residue code of length p

$\mathcal{RM}(r, m)$ Reed-Muller code of order r and length 2^m

$\mathcal{RS}(k, q)$ q -ary Reed-Solomon code of length $q - 1$ and dimension k

\mathcal{SIM}_m simplex code of length $2^m - 1$

$\Gamma = (V, E)$ graph with vertex set V and edge set E

$Tr(x)$ trace function

$P_j^n(x)$ Krawtchouk polynomial; superscript n may be omitted

$L_j^n(x)$ Lloyd polynomial; superscript n may be omitted

$H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ binary entropy of x , $0 \leq x \leq 1$

Contents

Preface	vii
Contents	ix
List of Symbols	xv
List of Tables	xxi
1 Introduction	1
1.1 Covering problems	2
1.2 Applications	10
2 Basic facts	15
2.1 Codes	15
2.2 The MacWilliams identities	24
2.3 Krawtchouk polynomials	27
2.4 Hamming spheres	32
2.5 Finite fields	40
2.6 Families of error-correcting codes	45
2.7 Designs, constant weight codes, graphs	52
2.8 Notes	57
3 Constructions	61
3.1 Puncturing and adding a parity check bit	62
3.2 Direct sum	63
3.3 Piecewise constant codes	64
3.4 Variations on the $(u, u + v)$ construction	66
3.5 Matrix construction	70
3.6 Cascading	72
3.7 Optimal short nonbinary codes	73
3.8 Simulated annealing and local search	79
3.9 Notes	80

4	Normality	85
4.1	Amalgamated direct sum	85
4.2	Normality of binary linear codes	94
4.3	Abnormal binary nonlinear codes	102
4.4	Normality of binary nonlinear codes	106
4.5	Blockwise direct sum	110
4.6	Notes	114
5	Linear constructions	119
5.1	Basic facts about linear covering codes	120
5.2	The case $R = 1$; examples of small codes	122
5.3	Saving more than one coordinate	127
5.4	Davydov's basic construction	129
5.5	Notes	143
6	Lower bounds	145
6.1	Bounds for the cardinality of the union of K spheres	146
6.2	Balanced codes	149
6.3	Excess bounds for codes with covering radius one	151
6.4	Excess bounds for codes with arbitrary covering radius	156
6.5	The method of linear inequalities	158
6.6	Table on $K(n, R)$	165
6.7	Lower bounds for nonbinary codes	170
6.8	Notes	177
7	Lower bounds for linear codes	181
7.1	Excess bounds for linear codes	181
7.2	Linear codes with covering radius two and three	184
7.3	Tables for linear codes	191
7.4	Notes	213
8	Upper bounds	215
8.1	Codes with given size and distance	216
8.2	Covering radii of subcodes	222
8.3	Covering radius and dual distance	226
8.4	Notes	235
9	Reed-Muller codes	237
9.1	Definitions and properties	238
9.2	First order Reed-Muller codes	241
9.3	Reed-Muller codes of order 2 and $m - 3$	247
9.4	Covering radius of Reed-Muller codes of arbitrary order	251
9.5	Notes	258

10 Algebraic codes	261
10.1 BCH codes: definitions and properties	262
10.2 2- and 3-error-correcting BCH codes	266
10.3 Long BCH codes	269
10.4 Normality of BCH codes	277
10.5 Other algebraic codes	279
10.6 Notes	281
11 Perfect codes	285
11.1 Perfect linear codes over \mathbb{F}_q	286
11.2 A nonexistence result	290
11.3 Enumeration of perfect binary codes	296
11.4 Enumeration of perfect codes over \mathbb{F}_q	307
11.5 Mixed codes	310
11.6 Generalizations of perfect codes	312
11.7 Notes	314
12 Asymptotic bounds	319
12.1 Covering radius of unrestricted codes	320
12.2 Greedy algorithm and good coverings	322
12.3 Covering radius of linear codes	324
12.4 Density of coverings	328
12.5 Coverings of small size	332
12.6 Bounds on the minimum distance	338
12.7 Covering radius as a function of dual distance	342
12.8 Packing radius <i>vs</i> covering radius	346
12.9 Notes	351
13 Weighted coverings	355
13.1 Basic notions	355
13.2 Lloyd theorem for perfect weighted coverings	357
13.3 Perfect weighted coverings with radius one	361
13.4 Weighted coverings and nonexistence results	365
13.5 Notes	368
14 Multiple coverings	371
14.1 Definitions	371
14.2 Perfect multiple coverings	373
14.3 Normality of multiple coverings	378
14.4 Constructions	381
14.5 Tables for multiple coverings	382
14.6 Multiple coverings of deep holes	385
14.7 Notes	389

15 Football pools	393
15.1 Constructions for mixed binary/ternary codes	394
15.2 Tables for mixed binary/ternary codes	397
15.3 On the early history of the ternary Golay code	401
15.4 Notes	402
16 Tilings	403
16.1 Preliminaries	403
16.2 A sufficient condition	405
16.3 Small tiles	406
16.4 Periodicity of tilings	409
16.5 Recursive decomposition of tilings	412
16.6 Tilings and perfect binary codes	415
16.7 Nonexistence results	417
16.8 Notes	420
17 Writing on constrained memories	423
17.1 Worst case coverings and WOMs	423
17.2 The error case	428
17.3 A model for correcting single errors	429
17.4 Single-error-correcting WOM-codes	430
17.5 Nonlinear WOM-codes	433
17.6 Notes	436
18 Subset sums and constrained memories	439
18.1 Cayley graphs	439
18.2 Subset sums	441
18.3 Maximal sum-free sets	446
18.4 Constrained memories (W^* Ms)	448
18.5 Translation-invariant constraints	449
18.6 Domatic number and reluctant memories	452
18.7 Defective memories	455
18.8 The error case	456
18.9 Notes	456
19 Heterodox coverings	461
19.1 Perfect coverings by L -spheres	461
19.2 Perfect coverings by spheres of two radii	467
19.3 Coverings by spheres all of different radii	470
19.4 Multicovering radius	472
19.5 Perfect coverings of a sphere and constant weight coverings . .	473
19.6 Notes	475