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

This book is printed on acid-free paper

Printed in The Netherlands

North-Holland Mathematical Library

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 Hämäläinen, Juha Honkala, Olivier Hudry, Osnat Keren, Ilia Krasikov, Tero Laihonen, 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 $\{1, 2, \ldots, n\}$

$:=$ 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

$\mathbb{Z}_q = \{0, 1, ..., q-1\}$ 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 $\mathbb{F}_q$

$\psi_{\mathbf{u}}(\mathbf{x})$ additive character of $\mathbb{F}_q$

Q arbitrary alphabet of size q

$\mathbf{a} = (a_1, a_2, \ldots, a_n) = (a_1 a_2 \ldots a_n) = a_1 a_2 \ldots a_n$, $\mathbf{b}_i = b_{i,1} \ldots b_{i,n}$, $\mathbf{c}, \ldots$ 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

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

1^n, 0^n all-1 or all-0 vector of length n

$1^{n \times m}$, $0^{n \times m}$ 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 $\mathbf{y}$

$\mathrm{supp}(\mathbf{x})$ 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

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

$\mathcal{BCH}_h(e, m)$ nonprimitive BCH code of length $(2^m - 1)/h$ and designed distance $2e + 1$

$\mathcal{GOP}(L, g)$ Goppa code with defining set L and polynomial g

$\mathcal{HAD}_n$ 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

$\mathcal{QR}(p)$ 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