

Syracuse University

## SURFACE

---

Electrical Engineering and Computer Science -  
Technical Reports

College of Engineering and Computer Science

---

11-1994

### Covering Radius 1985-1994

G. D. Cohen

S. N. Litsyn

Antoine C. Lobstein

H. F. Mattson Jr

Follow this and additional works at: [https://surface.syr.edu/eecs\\_techreports](https://surface.syr.edu/eecs_techreports)



Part of the [Computer Sciences Commons](#)

---

#### Recommended Citation

Cohen, G. D.; Litsyn, S. N.; Lobstein, Antoine C.; and Mattson, H. F. Jr, "Covering Radius 1985-1994" (1994).  
*Electrical Engineering and Computer Science - Technical Reports*. 150.  
[https://surface.syr.edu/eecs\\_techreports/150](https://surface.syr.edu/eecs_techreports/150)

This Report is brought to you for free and open access by the College of Engineering and Computer Science at SURFACE. It has been accepted for inclusion in Electrical Engineering and Computer Science - Technical Reports by an authorized administrator of SURFACE. For more information, please contact [surface@syr.edu](mailto:surface@syr.edu).

SU-CIS-94-9

**Covering Radius 1985-1994**

Gérard D. Cohen, Simon N. Litsyn,  
Antoine C. Lobstein, & H. F. Mattson, Jr.

November 1994

School of Computer and Information Science  
Syracuse University  
Suite 4-116, Center for Science and Technology  
Syracuse, NY 13244-4100

# COVERING RADIUS 1985–1994

Dedicated to Eugene A. Prange

**Gérard D. Cohen**

Ecole Nationale Supérieure des Télécommunications  
46 rue Barrault, 75634 Paris cédex 13, France  
Email: cohen@inf.enst.fr

**Simon N. Litsyn**

Dept. of Electrical Engineering-Systems  
Tel-Aviv University, Ramat-Aviv, 69978, Israel  
Email: litsyn@eng.tau.ac.il

**Antoine C. Lobstein**

Centre National de la Recherche Scientifique  
Ecole Nationale Supérieure des Télécommunications  
46 rue Barrault, 75634 Paris cédex 13, France  
Email: lobstein@inf.enst.fr

**H. F. Mattson, Jr.**

School of Computer and Information Science  
4-116 Center for Science & Technology  
Syracuse, New York 13244-4100, USA  
Email: jen@SUVVM.acs.syr.edu

**Abstract.** We survey important developments in the theory of covering radius during the period 1985-1994. We present lower bounds, constructions and upper bounds, the linear and nonlinear cases, density and asymptotic results, normality, specific classes of codes, covering radius and dual distance, tables, and open problems.

# 1 Introduction

## 1.1 Background

Interest in covering radius has grown markedly since about 1980. The topic has applications to problems of data compression, testing, and write-once memories. It is also interesting for its own sake. It is a fundamental geometric parameter of a code, characterizing its maximal error correcting capability in the case of minimum distance decoding. Although some of these applications are recent, others are old. Yet after the 1960 paper of Gorenstein, Peterson, and Zierler [78] showing that the double-error-correcting binary BCH code has covering radius 3, (though there were some papers on the football-pool problem), there was nothing on covering radius until the seminal paper [58] of Delsarte in 1973.

An earlier survey, [43], published in 1985, has seemingly contributed to the increase in the number of papers on this topic in the last decade. Covering radius has evolved into a subject in its own right, and we feel the need to give a summary of many works on covering codes that have appeared since [43].

### Plan of the paper

We discuss lower bounds in Section 2, mentioning several methods but especially linear programming and the method of excess. These methods usually improve on the sphere-covering bound.

In Section 3 we discuss asymptotic density of coverings when the length goes to infinity while the radius remains fixed.

In Section 4 we treat upper bounds for linear codes, focusing on the deficiency of a code, “worst” codes (useful in designing write-once memories), and Griesmer, optimum, and maximum codes.

Section 5 discusses upper bounds obtained from constructions. There are blockwise direct sums, amalgamated direct sums, variants on the  $u|u + v$  construction, and simulated annealing. This section closes with codes over mixed alphabets.

In Section 6 we discuss normality and some of its many offshoots, closing with the conjecture  $K(n + 2, t + 1) \leq K(n, t)$ .

Section 7 deals with specific classes of error correcting codes, among which are Reed-Muller, BCH and their duals, cyclic, binary self-dual and algebraic-geometric codes.

Section 8 is a brief account of relations between covering radius and dual distance.

Section 9, on generalizations of coverings, treats mixed, weighted, and multiple coverings.

In Section 10 we discuss the open problems of [43], add two new ones, and disprove a conjecture.

We provide extensive tables of bounds for coverings.

In our bibliography of some 265 items we have tried to include all papers bearing on the covering radius of block codes.

## 1.2 Nomenclature

$\mathbb{N}$  = set of all integers  $\geq 0$ ;  $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ .

$\mathbf{F} = \mathbf{F}_2 = \{0, 1\}$ ;  $\mathbf{F}_q = GF(q)$  = finite field of  $q$  elements.

For  $x \in \mathbf{F}_q^n$ ,  $\text{supp}(x) = \{i; x_i \neq 0\}$ .

$\text{wt}(x)$  or  $|x|$  = Hamming weight of vector  $x$  = cardinality of  $\text{supp}(x)$ .

For  $x, y \in \mathbf{F}_q^n$ ,  $\bar{x}, x \cap y, y \setminus x$  refer to the supports of vectors  $x$  and  $y$ .

For  $q \in \mathbb{N}$ ,  $\mathbf{E}_q$  denotes an arbitrary  $q$ -set (set of exactly  $q$  elements).

For  $x, y \in \mathbf{E}_q^n$ ,  $d(x, y)$  = the number of coordinate-places in which  $x$  and  $y$  are different.

It is the Hamming distance between  $x$  and  $y$ .

$(u|v)$  = concatenation of vectors  $u$  and  $v$ .

$\underline{1}, \underline{0}$  = all-1 or all-0 row, or column vector, or matrix of length or dimension determined by context.

$\underline{1}^n, \underline{0}^n$  = all-1 or all-0 vector of length  $n$ .

$G^t$  = transpose of matrix  $G$ .

For  $x \in \mathbf{E}_q^n$ ,  $B_t(x) = \{y \in \mathbf{E}_q^n; d(x, y) \leq t\}$ , and  $V_q(n, t) = |B_t(x)|$ ; subscript  $q$  may be dropped in the binary case.

A set  $C$  *t-covers* (or *covers* if there is no ambiguity) a set  $V$  if  $\forall x \in V, d(x, C) \leq t$ . A code  $C \subseteq \mathbf{E}_q^n$  has *covering radius*  $t$  if  $t$  is the least integer for which  $C$  *t-covers*  $\mathbf{E}_q^n$ . We also say that such  $C$  is a *t-covering* (or a *covering*).

$t(C)$  = covering radius of code  $C$ .

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

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

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

$d'(C)$  = dual distance of code  $C$  (when  $C$  is linear,  $d'$  and  $d^\perp$  coincide).

$[n, k, d]t$  = binary linear code of length  $n$ , dimension  $k$ , minimum distance  $d$ , covering radius  $t$ .

$(n, K)t$  = binary code of length  $n$ , cardinality  $K$ , covering radius  $t$ .

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

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

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

$K_q(n, t)$  = smallest cardinality of a  $q$ -ary code of length  $n$  and covering radius  $t$ ; subscript  $q$  may be dropped in the binary case.

$A[n, d]$  = maximal cardinality of a binary linear code of length  $n$  and minimum distance  $d$ .

$a[n, d] = \log_2 A[n, d]$ .

$A_q(n, d)$  = maximal cardinality of a  $q$ -ary code of length  $n$  and minimum distance  $d$ ; subscript  $q$  may be dropped in the binary case.

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

$g[k, d]$  = Griesmer lower bound on  $n[k, d]$ .

$A \oplus B$  = direct sum of codes  $A$  and  $B$ . ("DS")

$A \dot{\oplus} B$  = amalgamated direct sum of codes  $A$  and  $B$ . ("ADS")

$\binom{a}{b} = 0$  if  $b < 0$  or  $b > a$ , provided  $a \in \mathbb{N}$ .

$\lfloor \cdot \rfloor$  = floor function;  $\lfloor x \rfloor$  = largest integer  $\leq x$ .

$\lceil \cdot \rceil$  = ceiling function;  $\lceil x \rceil$  = least integer  $\geq x$ .

For  $x \in [0, 1]$ ,  $H(x)$  = binary entropy of  $x$ .

End of proof or end of statement given without proof is marked with  $\square$ .

## 2 Lower Bounds

Lower bounds on covering radius can be proved by counting arguments—e.g., the sphere-covering bound, below—or by nonexistence results. For example, if there is no  $[21, 5]_5$  code, then  $t[21, 5] \geq 6$ . We give here some ways of obtaining lower bounds on  $K(n, t)$ ,  $k[n, t]$ , or  $t[n, k]$ . The most powerful ones use a technique introduced in [250], the *excess* method, which consists of estimating the number of vectors that are covered by several codewords (see Section 2.5). Sections 2.1–2.5 deal primarily with binary *nonlinear* codes. Section 2.6 is devoted to binary *linear* codes, and we also give a brief comment on *q-ary* and *mixed* codes (Section 2.7)—in particular, ternary and mixed binary/ternary codes, which are linked to the so-called *football pool* problem.

Lower bounds derived in this section will be listed in Tables A, B and C. Table A gives bounds for  $K(n, t)$  ( $1 \leq n \leq 33, 1 \leq t \leq 10$ ); Table B gives bounds for  $t[n, k]$  ( $1 \leq n \leq 64, 1 \leq k \leq n$ ); and Table C gives bounds for  $K_3(n, t)$  ( $1 \leq n \leq 13, 1 \leq t \leq 3$ ).

### 2.1 Sphere-Covering Bound

The so-called *sphere-covering bound* states that if  $C$  is a code of length  $n$  and covering radius  $t$ , then the volume of a sphere of radius  $t$ , multiplied by the cardinality of  $C$ , must be at least equal to the number of elements in  $\mathbf{F}^n$ :

**Proposition 2.1** For  $n, t \in \mathbb{N}, n \geq t$ ,

$$K(n, t) \geq \frac{2^n}{V(n, t)}. \quad (2.1)$$

$\square$

**Proposition 2.2** For  $n, t \in \mathbb{N}, n \geq t$ ,

$$2^{k[n, t]} \geq \frac{2^n}{V(n, t)}. \quad (2.2)$$

$\square$

Proposition 2.2 also gives a lower bound on  $t[n, k]$  for all  $n, k \in \mathbb{N}$ , with  $n \geq k$ .

**Example 2.1**

$$K(21, 1) \geq \frac{2^{21}}{22} > 95325.$$

$$2^{k[13, 2]} \geq \frac{2^{13}}{92} > 89, \text{ so } k[13, 2] \geq 7, \text{ and } t[13, 6] \geq 3.$$

## 2.2 Using Embedded Codes

The basic idea of [47] is that when constructing an  $(n, K)t$  code  $C$ , the most favorable case is to consider a maximal subcode  $C_0$  with minimum distance at least  $2t + 1$  (hence each codeword in  $C_0$  covers  $V(n, t)$  distinct vectors), and to complete  $C$  with codewords that can still cover up to  $V(n, t) - \binom{2t}{t}$  distinct vectors, not yet covered by  $C_0$ . So, if  $A(n, d)$  denotes the maximal cardinality of a (binary) code of length  $n$  and minimum distance  $d$  (with the convention that  $A(n, d) = 1$  if  $d > n$ ), we have the following result:

**Proposition 2.3** [47] For  $n, t \in \mathbb{N}, n \geq t$ ,

$$K(n, t) \geq \frac{2^n - A(n, 2t + 1) \binom{2t}{t}}{V(n, t) - \binom{2t}{t}}, \quad (2.3)$$

provided the denominator is positive. □

Several embedded codes can be used, leading to the following result:

**Proposition 2.4** [47] For  $n, t \in \mathbb{N}, n \geq t$ ,

$$K(n, t) \geq \frac{2^n - 2A(n, 2t + 1) \binom{2t}{t}}{V(n, t) - \frac{3}{2} \binom{2t}{t}}, \quad (2.4)$$

provided the denominator is positive. □

Neither (2.3) nor (2.4) is always better than the other. An upper bound on  $A(n, 2t + 1)$  may be used if the exact value is not known.

**Example 2.2**  $A(9, 3) \leq 40$  [166], so  $K(9, 1) \geq \frac{2^9 - 2 \cdot 40}{10 - 2} = 54$ .

## 2.3 Balanced Codes and Induction

This method, most efficient for codes with a small number of words, led to the following results:

**Proposition 2.5** [47] For  $t \geq 1, K(2t + 2, t) \geq 4$  and  $K(2t + 3, t) \geq 7$ . □

**Proposition 2.6** [102] For  $t \geq 4, K(2t + 4, t) \geq 8$ . □

A code  $C$  containing  $K$  codewords is said to be *balanced* if, in each coordinate position, there are either  $\lfloor K/2 \rfloor$  0's and  $\lceil K/2 \rceil$  1's, or vice versa. The proofs of Propositions 2.5 and 2.6, by induction on  $t$ , are based on the fact that codes with length  $n$ , covering radius  $t$ , and containing  $K(n, t)$  words (i.e., *optimal covering codes*) cannot be too unbalanced (and it is conjectured in [47, Section B] that among optimal codes there is at least one that is balanced).

## 2.4 Linear Programming

The idea is to construct a linear system of inequalities, leading to the linear programming problem of minimizing the cardinality of a code under these linear constraints. For instance, a code with covering radius 1 must satisfy the following  $n + 1$  inequalities, where  $A_i = A_i(u)$  ( $0 \leq i \leq n$ ) denotes the number of codewords at distance  $i$  from an arbitrary vector  $u$ , with the convention that  $A_j = 0$  for  $j < 0$  or  $j > n$ :

$$(n - i + 1)A_{i-1} + A_i + (i + 1)A_{i+1} \geq \binom{n}{i}. \quad (2.5)$$

For covering radius 2, these become

$$\begin{aligned} \binom{n - i + 2}{2} A_{i-2} + (n - i + 1)A_{i-1} + (1 + in - i^2)A_i + (i + 1)A_{i+1} \\ + \binom{i + 2}{2} A_{i+2} \geq \binom{n}{i}. \end{aligned} \quad (2.6)$$

Other inequalities can be thought of. The goal is then to minimize  $|C| = \sum_{0 \leq i \leq n} A_i$ . Of course, this idea is usually applied to small values of  $n$ .

## 2.5 The Method of Counting Excess

This method has led to many improvements on lower bounds for  $K(n, t)$  [250]. As we said in the introduction to Section 2, the idea is to estimate the number of vectors in  $\mathbf{F}^n$  that are covered by several spheres of radius  $t$  centered at the codewords. We shall state the two main results of [250] and give a sketch of the proof for the first one.

**Proposition 2.7** *For  $n, t \in \mathbb{N}, n > t$ ,*

$$K(n, t) \geq \frac{(n - t + \epsilon)2^n}{(n - t)V(n, t) + \epsilon V(n, t - 1)}, \quad (2.7)$$

where

$$\epsilon = (t + 1) \left\lceil \frac{n + 1}{t + 1} \right\rceil - (n + 1). \quad (2.8)$$

**Proposition 2.8** *For  $n, t \in \mathbb{N}, n \geq 2t$ ,*

$$K(n, t) \geq \frac{(V(n, 2) - \frac{1}{2}(t + 2)(t - 1) + \epsilon) 2^n}{(V(n, 2) - \frac{1}{2}(t + 2)(t - 1)) V(n, t) + \epsilon V(n, t - 2)} \quad (2.9)$$

where

$$\epsilon = \binom{t + 2}{2} \left\lceil \binom{n - t + 1}{2} / \binom{t + 2}{2} \right\rceil - \binom{n - t + 1}{2}. \quad (2.10)$$

□



If  $\epsilon = 0$ , (2.7) or (2.9) is the sphere-covering bound. Neither (2.7) nor (2.9) is always better than the other.

For  $t = 1$ ,  $n$  even, (2.7) reads

$$K(n, 1) \geq \frac{2^n}{n} \quad (2.11)$$

instead of

$$K(n, 1) \geq \frac{2^n}{n+1} \quad (2.12)$$

given by the sphere-covering bound. When  $n = 2^r$ , (2.7) leads to  $K(2^r, 1) \geq 2^{2^r-r}$  and so, because of Hamming codes:

$$K(2^r, 1) = 2^{2^r-r}. \quad (2.13)$$

**Sketch of the proof of Proposition 2.7.** Let  $C$  be a code of length  $n$  with covering radius  $t$ , and let  $A$  be the set of vectors at distance exactly  $t$  from  $C$ . Obviously,

$$|C|V(n, t-1) + |A| \geq 2^n. \quad (2.14)$$

Let  $Z_i = \{z \in \mathbb{F}^n; z \text{ is covered by exactly } i+1 \text{ codewords}\}$  for  $i = 0, 1, \dots$ , and  $Z = \bigcup_{i \geq 0} Z_i = \{z \in \mathbb{F}^n; z \text{ is covered by at least two codewords}\}$ . Let  $V$  be a subset of  $\mathbb{F}^n$ ; the excess of  $C$  on  $V$  is defined by  $E(V) = \sum_{i \geq 0} i|Z_i \cap V|$  (i.e., an element of  $V$  that is covered  $i+1$  times by  $C$  contributes  $i$  to  $E(V)$ ).

One then shows that if  $a \in A$ , then  $E(B_1(a)) \equiv -|B_1(a)| \pmod{t+1}$ , and so

$$E(B_1(a)) = \sum_{i \geq 0} i|Z_i \cap B_1(a)| \geq \epsilon \text{ for all } a \in A. \quad (2.15)$$

For  $z \in Z$ , there exist at least two distinct codewords,  $c$  and  $d$ , such that  $d(z, c) \leq t$  and  $d(z, d) \leq t$ ; hence  $|A \cap B_1(z)| \leq n+1-\lambda$ , where  $\lambda = |B_1(z) \cap (B_{t-1}(c) \cup B_{t-1}(d))|$ . The next step consists of proving that  $\lambda \geq t+1$ . The case  $t = 1$  is trivial; if  $t \geq 2$ ,  $B_{t-1}(c) \cap B_{t-1}(d)$  may be nonempty. Set  $d_1 = d(z, c)$ ,  $d_2 = d(z, d)$ ; without loss of generality, one of the following four cases holds: 1)  $d_1 = d_2 = t$ , 2)  $d_1 = t-1, d_2 = t$ , 3)  $d_1 = d_2 = t-1$ , 4)  $d_1 \leq t-2, d_2 \leq t$ . Then, in cases 1), 2), and 3), we may say that  $d(c, d) = 2, 1$ , and  $2$ , respectively, is the worst case; in these three configurations for  $z, c$ , and  $d$ , we find  $\lambda \geq t+1$ . In case 4),  $B_1(z) \subseteq B_{t-1}(c)$ , so  $\lambda \geq n+1 \geq t+1$ .

This leads to

$$|A \cap B_1(z)| \leq n-t, \text{ for all } z \in Z. \quad (2.16)$$

By (2.14), (2.15), (2.16) and  $|C|V(n, t) - \sum_{i \geq 0} i|Z_i| = 2^n$ , we get

$$\begin{aligned} \epsilon(2^n - |C|V(n, t-1)) &\leq \epsilon|A| \leq \sum_{a \in A} \sum_{i \geq 0} i|Z_i \cap B_1(a)| \leq \sum_{i \geq 0} i \sum_{z \in Z_i} |A \cap B_1(z)| \\ &\leq \sum_{i \geq 0} i(n-t)|Z_i| = (n-t)(|C|V(n, t) - 2^n), \end{aligned}$$

and finally

$$|C| \geq \frac{(n-t+\epsilon)2^n}{(n-t)V(n,t) + \epsilon V(n,t-1)}.$$

□

Proposition 2.8 is proved by estimating the excess of  $C$  on spheres of radius two instead of radius one as for Proposition 2.7.

A further study of the method of excess in the case  $n = 11, t = 3$  [119] gives one more small improvement:  $K(11, 3) \geq 12$ .

**Example 2.3**  $n = 12, t = 1$ ; Proposition 2.7 yields  $\epsilon = 1$  and  $K(12, 1) \geq \frac{12 \cdot 2^{12}}{11 \cdot 13 + 1} > 341$ , whereas Proposition 2.8 yields  $\epsilon = 0$  and  $K(12, 1) \geq \frac{2^{12}}{13} > 315$ .

$n = 11, t = 1$ ; Proposition 2.7 yields  $\epsilon = 0$  and  $K(11, 1) \geq \frac{2^{11}}{12} > 170$ , whereas Proposition 2.8 yields  $\epsilon = 2$  and  $K(11, 1) \geq \frac{(67+2) \cdot 2^{11}}{67 \cdot 12} > 175$ .

Further improvements on Propositions 2.7 and 2.8 can be found in [102], using results on  $f(n, p)$ , the minimal cardinality of any constant-weight- $p$  binary code  $C$  of length  $n$  ( $n \geq p \geq 2$ ) satisfying  $\forall x \in \mathbf{F}^n$  with  $|x| = 2, \exists c \in C$  such that  $\text{supp}(x) \subseteq \text{supp}(c)$ . (In other words, if codewords are seen as subsets of an  $n$ -element set  $V$ ,  $C$  is a collection of  $p$ -element subsets of  $V$  such that every 2-subset (sometimes “pair” in the literature) of  $V$  is contained in at least one element of  $C$ .) The idea is to have a closer look, by dividing them into several classes, at the points that are covered several times, and get a better estimate for some of them. Propositions 2.9 and 2.10 study excess on spheres of radius 1 and 2, respectively.

**Proposition 2.9** [102] For  $t \geq 2, n \geq 2t+1$  and  $\epsilon = (t+1)\lceil(n+1)/(t+1)\rceil - (n+1) \leq t-1$ ,

$$K(n, t) \geq \frac{(\rho + \epsilon)2^n}{\rho V(n, t) + \epsilon V(n, t-1)}, \quad (2.17)$$

$$\text{where } \rho = \begin{cases} n-3+2/n, & \text{if } t=2 \\ n-t-1, & \text{if } t \geq 3 \end{cases}. \quad (2.18)$$

□

This inequality does not give new results for  $t = 1$  or  $\epsilon = t$ , but when  $t > 1$  and  $\epsilon < t$ , it is always better than Proposition 2.7.

**Proposition 2.10** [102] If  $n \geq 2t+1$ , and if

$$\begin{aligned} \text{as in (2.10), } \epsilon &= \binom{t+2}{2} \left[ \binom{n-t+1}{2} / \binom{t+2}{2} \right] - \binom{n-t+1}{2}, \\ \lambda &= \epsilon + \left( f(n-t+1, t+2) - \left[ \binom{n-t+1}{2} / \binom{t+2}{2} \right] \right) \binom{t+2}{2}, \end{aligned} \quad (2.19)$$

$$\mu_0 = 2 + n(t-2) - \binom{t-2}{2}, \quad (2.20)$$

$$\mu_1 = 2t^2 - t + 1 - \lambda, \quad (2.21)$$

$$\text{and } \mu = \begin{cases} \mu_1, & \text{if } t = 1 \\ \min(\mu_0, \mu_1), & \text{if } t \geq 2 \end{cases} \quad (2.22)$$

then

$$K(n, t) \geq \frac{(V(n, 2) - \mu + \lambda) 2^n}{(V(n, 2) - \mu) V(n, t) + \lambda V(n, t - 2)}. \quad (2.23)$$

□

When  $f(n - t + 1, t + 2)$  is not known, a lower bound can be used in (2.19). Proposition 2.10 gives at least as good results as Proposition 2.8.

Propositions 2.9 and 2.10 gave many small improvements on lower bounds for  $K(n, t)$ .

**Example 2.4**  $n = 13, t = 2$ ; by Proposition 2.9,  $\epsilon = 1, \rho = 10 + 2/13$ , and

$$K(13, 2) \geq \frac{\left(11 + \frac{2}{13}\right) \cdot 2^{13}}{\left(10 + \frac{2}{13}\right) \cdot 92 + 14} > 96.$$

Now  $f(12, 4) = 12$  [176], and by Proposition 2.10,  $\epsilon = 0, \lambda = 6, \mu_0 = 2, \mu_1 = 1, \mu = 1$ , and

$$K(13, 2) \geq \frac{(92 + 5) \cdot 2^{13}}{(92 - 1) \cdot 92 + 6} > 94.$$

$n = 14, t = 4$ ; by Proposition 2.9,  $\epsilon = 0$ , and  $K(14, 4) \geq 2^{14}/1471 > 11$ . But  $f(11, 6) = 6$  [176], and by Proposition 2.10,  $\epsilon = 5, \lambda = 35, \mu_0 = 24, \mu_1 = -6, \mu = -6$ , and

$$K(14, 4) \geq \frac{(106 + 6 + 35) \cdot 2^{14}}{(106 + 6) \cdot 1471 + 35 \cdot 106} > 14.$$

Finally, studying some special cases (such as  $n \equiv 5 \pmod{6}$  and  $t = 1$ ) can lead to further improvements (see [107], [254] or [110]).

Association schemes can be used together with the excess method (on spheres of radius 2) and the function  $f(n, p)$  (covering 2-subsets by  $p$ -subsets), yielding the following proposition, which is the main result of [265].

**Proposition 2.11** *If  $m_1$  and  $m_2$  are two positive numbers, and if  $m_0(m_1, m_2) = \min_{k \geq 1} \{km_1 + f(n - kt + 1, t + 2)m_2\}$ , then*

$$K(n, t) \geq \frac{m_0(m_1, m_2) 2^n}{\sum_{0 \leq i \leq t-2} m_0(m_1, m_2) \binom{n}{i} + m_1 \left( \binom{n}{t-1} + \binom{n}{t} \right) + m_2 \left( \binom{n}{t+1} + \binom{n}{t+2} \right)}. \quad (2.24)$$

□

**Example 2.5**  $n = 10, t = 2$ ; let  $m_1 = 3$  and  $m_2 = 1$ . Then,  $\min_{k \geq 1} \{3k + f(11 - 2k, 4)\} = \min_{k \geq 1} \{3 + f(9, 4), 6 + f(7, 4), 9 + f(5, 4)\} = \min\{11, 11, 12\} = 11$  [176]. So  $m_0(m_1, m_2) = 11$ , and

$$K(10, 2) \geq \frac{11 \cdot 2^{10}}{11 + 3 \cdot (10 + 45) + (120 + 210)} > 22.$$

Again, this lower bound improved on many entries of the table of  $K(n, t)$ ; furthermore, refinements can be brought to (2.24) (see [152], [265], [266]). In [266], Zhang and Lo analyze the covering of “triples” (3-subsets). They obtain 20 improvements in lower bounds on  $t[n, k]$ , such as  $t[29, 10] \geq 7$  and  $t[63, 16] \geq 16$  (vs. prior bounds 6 and 15, resp.), and many improved lower bounds on  $K(n, t)$ .

## 2.6 The Linear Case

Almost all lower bounds given above are derived for nonlinear codes. We now look at the linear case, where it must be said that most of the best-known lower bounds on  $k[n, t]$  or  $t[n, k]$  are nothing more than the sphere-covering bound. New lower bounds are usually established via proof of nonexistence of an  $[n, k]_{t_0}$  code for specific values of  $n, k$ , and  $t_0$ . (That would prove  $t[n, k] > t_0$ .) By contrast, the nonlinear case admits general lower bounds on  $K(n, t)$ . This is why we shall not elaborate in this section on the plethora of ad hoc proofs.

### 2.6.1 A Result Derived From the Nonlinear Case

**Proposition 2.12** [250, (3)] *If for some  $n, t_0$ , and  $s$ , we have  $K(n, t_0) > 2^s$ , then  $t[n, s] > t_0$ .*  $\square$

This obvious result allows improvements in the table of  $t[n, k]$ . For example, in [43] and [79], the entry for  $t[23, 6]$  was “6 – 7.” Now that  $K(23, 6)$  is known [250] to be greater than 64, we can say that  $t[23, 6] = 7$ .

### 2.6.2 The Case of Low Dimension: $k \leq 5$

The 1985 survey [43] states that:  $t[n, 1] = \lfloor n/2 \rfloor$  for  $n \geq 1$ ;  $t[n, 2] = \lfloor (n-1)/2 \rfloor$  for  $n \geq 2$ ;  $t[n, 3] = \lfloor (n-2)/2 \rfloor$  for  $n \geq 3$ ;  $t[n, 4] = \lfloor (n-4)/2 \rfloor$  for  $n \geq 4$  and  $n$  even,  $t[5, 4] = 1$ ,  $t[n, 4] = \lfloor (n-4)/2 \rfloor$  for  $n = 7, 9, 11, 13, 15$  or  $17$ , and  $t[n, 4] = \lfloor (n-4)/2 \rfloor$  or  $\lfloor (n-3)/2 \rfloor$  for  $n \geq 19$  and  $n$  odd;  $t[n, 5] \leq \lfloor (n-5)/2 \rfloor$  for  $n \geq 5$  and  $n \neq 6$ ,  $t[6, 5] = 1$ .

In [79] the exact values of  $t[n, k]$  are given for  $k \leq 5$ :  $t[n, 4] = \lfloor (n-4)/2 \rfloor$  for  $n \geq 4$  and  $n \neq 5$  (improving on upper bounds by construction (see Section 5.3, Example 5.2));  $t[n, 5] = \lfloor (n-5)/2 \rfloor$  for  $n \geq 5$  and  $n \neq 6$  (improving on lower bounds by an ad hoc proof, with the help of a Cray-1 computer;  $t[12, 6] \geq 3$  also has been proved in the same way).

### 2.6.3 Particular Values of $k$ and $n$ , ad hoc Proofs

Linear inequalities for linear binary covering codes, analogous to the Delsarte-MacWilliams inequalities for error-correcting codes, can be derived by involving the Lloyd polynomials

[29]. In spite of the fact that these inequalities generalize the sphere-covering bound, they do not lead directly to new lower bounds for  $t[n, k]$ , and some more specific investigations have to be made.

Inequalities derived from the Griesmer bound and the Johnson bound, together with the study of the weights of the dual code, can also lead to new lower bounds on  $t[n, k]$  for some values of  $n$  and  $k$  [24], [267].

Other ad hoc investigations have been made in [22], [119], [122], [216], [217], [259].

#### 2.6.4 Other Results

Some explicit formulas can be found. For instance, a special study of the cases  $n + 1 = p(t + 1) - \tau$  ( $0 \leq \tau < t + 1, p > 2$  odd), and  $n + 1 = p(t + 1) - 1$  ( $p > 2$  even) [121], again using the excess method adapted to the linear case, leads to formulas for a lower bound on  $k[n, t]$  (hence on  $t[n, k]$ ), involving the minimum distance of the code. A lower bound on the minimum distance of an optimal covering code then allows us to improve several lower bounds on  $t[n, k]$ . For instance, if  $C$  is an  $[n, k, d]$  code and if  $n + 1 = p(t + 1)$  with  $p > 2$  odd, then

$$2^{n-k} \leq V(n, t - 1) + \frac{(n + 1 - t - \lceil d/2 \rceil) \binom{n}{t} + (t + 1)}{n + 2 - \lceil d/2 \rceil}. \quad (2.25)$$

**Example 2.6**  $n = 19, t = 3$  (hence  $p = 5$ );  $\lceil d/2 \rceil$  is at least 2, and  $2^{19-k} \leq 191 + \frac{15 \cdot 969 + 4}{19} \leq 956$ , so  $k \geq 10 : t[19, 9] \geq 4$ .

Struik [235] has improved several lower bounds on  $t[n, k]$  or  $\ell(m, t)$ , the binary length function of [24] (for more on the length function, see Section 10). He presented some of these results earlier [232], [233]. He begins by extending Proposition 3.1. We illustrate his approach for covering radius 2.

Let  $C$  be an  $[n, m]$  code for which  $t(C^\perp) = 2$ . Then each nonzero weight  $w$  of  $C$  satisfies

$$w 2^{n-w-m+1} \geq K(n - w, 1).$$

Moreover, for a given weight  $w$ , if no such code  $C$  has a vector of weight  $w$ , then no such code  $C$  has a vector of weight  $n + 1 - w$ . Together with the bound  $w(n + 1 - w) \geq 2^{m-1}$  of [24, Lemma 4.6], these results narrow the possible weights of  $C$  enough to allow ad hoc arguments to prove nonexistence of  $C$  in some specific cases. For example, he proves there is no  $[18, 7]$  code  $C$  with  $t(C^\perp) = 2$ . Thus  $t[18, 11] \geq 3$ , or  $\ell(7, 2) \geq 19$ . Although this bound was first proved with the help of a computer [259], Struik's proof is brief and self-contained. (The bound  $\ell(7, 2) \leq 19$  is known [79], so  $\ell(7, 2) = 19$ .)

He proves a conjecture of [24]:  $\ell(2m - 1, 2) \geq 2^m + 1$  for all  $m \geq 3$ .

He has several other bounds on  $\ell$  for covering radii 2 and 3 and specific values of  $n$  and  $m$ . These include a two-page proof that  $\ell(6, 2) = 13$  ( $t[12, 6] = 3$ ), i.e., there is no  $[12, 6]$  code with covering radius 2. (cf. 2.6.2.) This was first proved by computer [79] and later at

length without a computer [24]. He also has a lengthy proof that  $\ell(8, 2) \geq 25$ , i.e., that no  $[24, 16]_2$  code exists.

For linear and nonlinear codes, numerical results derived from Sections 2.1–2.6 can be found in two tables: Table A gives bounds for  $K(n, t)$  with  $1 \leq n \leq 33$  and  $1 \leq t \leq 10$ ; Table B gives bounds for  $t[n, k]$  for  $1 \leq n \leq 64$  and  $1 \leq k \leq n$ .

## 2.7 Codes With $q$ -ary or Mixed Alphabets

The search for the smallest cardinality of a (linear) code with length  $n$  and covering radius  $t$ , or the smallest covering radius of a linear code with length  $n$  and dimension  $k$ , can be extended to codes over a  $q$ -ary alphabet, leading to the obvious notation  $K_q(n, t)$ ,  $k_q[n, t]$  and  $t_q[n, k]$ . Codes with mixed alphabets (different alphabets for different coordinates) can also be considered (cf. Section 9).

We shall give some general results for  $q$ -ary and mixed codes, and then focus on ternary and mixed binary/ternary codes, which are linked to the well-known *football pool* problem, which we now define.

Suppose  $n$  football matches are to be played. A *bet* on these matches consists of a prediction of the winner of each of the  $n$  matches. Thus a bet is a ternary [binary]  $n$ -vector if ties are [not] possible. If we set a threshold  $t \geq 1$ , then the problem is to choose a set of bets so as to be sure that one of these bets has at least  $n - t$  winners. We see that the bets should constitute a code of covering radius  $t$ . ( $K_3(n, t)$  represents the minimal number of predictions necessary to guarantee, for  $n$  matches, that at least one prediction has at most  $t$  wrong results; mixed binary/ternary codes represent the case when, for some matches, only two results are considered: if a strong team plays at home against a weak team—you can imagine that it will not lose; if you think that it can only win, then shorten the length of the code by 1!).

We shall give in Table C the bounds for  $K_3(n, t)$  ( $1 \leq n \leq 13, 1 \leq t \leq 3$ ). Tables of lower bounds for  $K_3(n, t)$  ( $1 \leq n \leq 14, 1 \leq t \leq 9$ ),  $K_4(n, t)$  ( $1 \leq n \leq 10, 1 \leq t \leq 7$ ) and  $K_5(n, t)$  ( $1 \leq n \leq 9, 1 \leq t \leq 7$ ) can be found in [32], and the same lower bounds appeared in [191], which is devoted only to improving upper bounds on  $K_q(n, t)$ . More recent tables of lower bounds for  $K_3(n, 1)$  ( $1 \leq n \leq 14$ ),  $K_4(n, 1)$  ( $1 \leq n \leq 10$ ) and  $K_5(n, 1)$  ( $1 \leq n \leq 9$ ) are given in [80], and for  $K_3(n, t)$  ( $1 \leq n \leq 14, 1 \leq t \leq 8$ ) in [160] and [254] (with also upper bounds). A table of lower bounds for mixed binary/ternary codes was published in both [156] and [157] (for  $n = T + B \leq 13$  and  $t \leq 3$ ); a table of upper bounds for mixed binary/ternary codes can be found in [199] (for  $T + B \leq 13$  and  $t \leq 3$ ). For the same parameters, a new table of upper bounds will appear in [200].

### 2.7.1 The $q$ -ary Case

The sphere-covering bound reads in the  $q$ -ary case:

**Proposition 2.13** For  $n, t \in \mathbb{N}, n \geq t, q \in \mathbb{N}, q \geq 2$ ,

$$K_q(n, t) \geq \frac{q^n}{V_q(n, t)}. \quad (2.26)$$

□

As in the binary case, linear programming (see [163] for the ternary case) or counting excess [32], [253] can be used to improve on the sphere-covering bound. The latter method leads, through heavy complications, to the following results:

$$\text{Assume that } q > 2, \text{ and let } \tau = \left\lceil \frac{n}{t} \right\rceil - 1, \quad (2.27)$$

$$\epsilon_i = (t+1) \left\lceil \frac{(q-1)(n-ti-t)}{t+1} \right\rceil - (q-1)(n-ti-t) + i, \text{ for } 0 \leq i < \tau, \quad (2.28)$$

$$\epsilon_\tau = (q-1) \left( t \left\lceil \frac{n}{t} \right\rceil - n \right) + \tau, \quad (2.29)$$

$$\text{and } \epsilon = \min_{1 \leq i \leq \min\{t, \tau\}} \{\epsilon_i\}. \quad (2.30)$$

$$\text{If } t = 1, \text{ let } \rho = (q-1)n - 1, \quad (2.31)$$

$$\text{and if } t > 1, \text{ let } \rho = \max\{\rho_1, \rho_2\}, \quad (2.32)$$

where  $\rho_1 = (q-1)n - 2t + 1 + \left\lfloor \frac{\epsilon-1}{q-1} \right\rfloor + \epsilon_0 - \epsilon$ , and  $\rho_2 = (q-1)(n-1) - 1 + \frac{q}{2(q-1)(n-1)+q}$  if  $t = 2$ ,  $\rho_2 = (q-1)(n-t+1)$  if  $t > 2$ .

Then:

**Proposition 2.14** [32] *For  $n, q, t \in \mathbb{N}, n \geq 2, q > 2, n > t$ ,*

$$K_q(n, t) \geq \frac{(\rho + \epsilon_0)q^n}{\rho V_q(n, t) + \epsilon_0 V_q(n, t-1)}, \quad (2.33)$$

where  $\rho$  is as in (2.31) or (2.32), and  $\epsilon_0$  is as in (2.28). □

Proposition 2.14 is proved by estimating the excess of a covering code on spheres of radius one. The study of spheres of radius two gives [32, Th. 4], the statement of which requires too much notation to be given here.

**Example 2.7**  $q = 3, n = 7, t = 2$ ; then  $\tau = 3, \epsilon_0 = 2, \epsilon_1 = 1, \epsilon_2 = 3, \epsilon = 1, \rho_1 = 12, \rho_2 = 11 + \frac{3}{27}, \rho = 12$ , and  $K_3(7, 2) \geq \frac{14 \cdot 3^7}{12 \cdot 99 + 2 \cdot 15} > 25$ .

The method presented in [80] can be seen as counting excess on  $q$ -ary sets. Restricted to the binary case, it also gives several new lower bounds.

The technique using embedded codes can be extended to the  $q$ -ary case [254], and Proposition 2.3 generalized; if  $A_q(n, d)$  denotes the maximal cardinality of a  $q$ -ary code of length  $n$  and minimum distance  $d$  (with the convention that  $A_q(n, d) = 1$  if  $d > n$ ), then:

**Proposition 2.15** For  $n, t \in \mathbb{N}, n \geq 2t$ ,

$$K_q(n, t) \geq \frac{q^n - A_q(n, 2t+1) \binom{2t}{t}}{V_q(n, t) - \binom{2t}{t}}. \quad (2.34)$$

□

As in the binary case, an upper bound on  $A_q(n, 2t+1)$  will be used when the exact value is not known. For instance, a table of lower and upper bounds on  $A_3(n, d)$  can be found in [245].

**Example 2.8**  $A_3(8, 5) \leq 30$  [245], so  $K_3(8, 2) \geq \frac{3^8 - 6 \cdot 30}{129 - 6} > 51$ .

Before closing this section on  $q$ -ary codes, let us mention that the ideas governing Proposition 2.11 can more or less be extended to the ternary case [160].

### 2.7.2 Mixed Codes

A mixed code is a subset  $C$  of some cartesian product  $V = \mathbf{E}_{q_1} \times \mathbf{E}_{q_2} \times \cdots \times \mathbf{E}_{q_n}$ . With  $t = t(C)$ , the sphere-covering bound is now

$$|C| \geq \frac{\prod_{1 \leq i \leq n} q_i}{1 + \sum_{1 \leq j \leq t} \sum_{1 \leq i_1 < \dots < i_j \leq n} (q_{i_1} - 1) \cdots (q_{i_j} - 1)}. \quad (2.35)$$

The case  $q_1 = q_2 = \dots = q_T = 3, q_{T+1} = q_{T+2} = \dots = q_{T+B=n} = 2$ , or mixed binary-ternary case, is linked to the football-pool problem and has been studied in more detail. In this case, the volume of the sphere of radius  $t$  is equal to

$$V(T, B, t) = \sum_{0 \leq j \leq t} \sum_{0 \leq i \leq j} \binom{T}{i} 2^i \binom{B}{j-i},$$

and, using the obvious notation  $K(T, B, t)$ , the sphere-covering bound reads:

$$K(T, B, t) \geq \frac{3^T 2^B}{V(T, B, t)}. \quad (2.36)$$

Again, the excess method can give improvements on the sphere-covering bound [156]:

**Proposition 2.16** If  $C \subset \mathbf{F}_3^T \cdot \mathbf{F}_2^B$  has covering radius  $t$ , and if for  $j = 1, 2, \dots, t, m_j$  is the least nonnegative integer such that  $m_j \equiv 1 + 2T + B + j \pmod{t+1}$ , then

$$|C| \geq \frac{(1 + 2T + B - t) 3^T 2^B}{(1 + 2T + B - t) V(T, B, t) - \sum_{1 \leq j \leq t} \binom{T}{m_j} \binom{B}{t - m_j} 2^{m_j}}. \quad (2.37)$$

□



For  $t = 1$ , this leads to: if  $B$  is odd,  $|C| \geq \frac{(2T+B)3^T 2^B}{(2T+B)(1+B+2T)-2T}$ , and if  $B$  is even,  $|C| \geq \frac{(2T+B)3^T 2^B}{(2T+B)(1+B+2T)-B}$ , a result that is also stated in [253].

For  $t > 1$ , (2.37) has still been improved (see [156] or [157]), through some complications.

For  $t$  up to 3 and small lengths ( $n = 6, 7, 8$ ), see [143].

## 2.8 Lower Bounds Through Discrepancy

Let  $K$  be a positive integer and let  $L$  be a subset of  $\mathbf{F}^n$  of size  $K$ . For  $x \in \mathbf{F}^n$ , set

$$f(x, L) := \max_{v \in L} ||v \cap x| - |v \cap \bar{x}||.$$

(Here the outer vertical bars mean absolute value, and the inner ones mean cardinality; we identify vectors with their supports.) We define the *discrepancy* of  $L$  by the formula

$$\text{disc}(L) := \min_{x \in \mathbf{F}^n} f(x, L),$$

and finally we define  $f(K)$  as

$$f(K) := \max_{L, |L|=K} \text{disc}(L).$$

Since  $f(x, L) = f(\bar{x}, L)$ , we assume  $|x| \geq n/2$ . And since  $|v \cap x| - |v \cap \bar{x}| = |x| - |x + v|$ , we see that for all  $v \in L$ ,

$$|x + v| \geq n/2 - f(K).$$

Using estimates on  $f(K)$  from [8] and [189], we have the following bounds on  $t(n, K)$ .

*Olson-Spencer:* [189]

$$t(n, K) \geq n/2 - (2K)^{1/2} \log_e 2K. \quad (2.38)$$

*Beck-Fiala:* [8]

$$t(n, K) \geq n/2 - 8(2K \log_e 2K)^{1/2}. \quad (2.39)$$

Yet another bound on the discrepancy  $\text{disc}(L)$  can be found in [3]:  $\text{disc}(L) \leq (2n \log_e 2K)^{1/2}$ .

Thus

*Alon-Spencer:* [3]

$$t(n, K) \geq n/2 - (2n \log_e 2K)^{1/2}. \quad (2.40)$$

For  $n < 64K$ , (2.40) outperforms (2.39). For  $n < K \log_e 2K$ , (2.40) outperforms (2.38).

## 3 Density of Coverings

For a  $q$ -ary code  $C$  of length  $n$  and covering radius  $t$ , let us define its *density* by

$$\mu(C) = \frac{|C|V_q(n, t)}{q^n}.$$

$\mu(C)$  is the average over all vectors  $x$  in  $\mathbf{F}_q^n$  of the number of codewords within distance  $t$  of  $x$ . We set  $\mu_n(q, t)$  to be the minimal density over all such codes in  $\mathbf{F}_q^n$ .

Let us denote by  $\underline{\mu}(q, t)$  and  $\mu(q, t)$ , respectively, the lim inf and lim—when it exists—of  $\mu_n(q, t)$  when  $n$  goes to infinity. In the binary case we shall omit  $q$ . Thus  $\mu(2, t) = \mu(t)$ .

That  $\mu(1) = 1$  was conjectured in [10]. The more general result  $\mu(q, 1) = 1$  for  $q$  a prime power is proved by Kabatianskii and Panchenko [134] and extended by Panchenko [202] to such  $q$  that there exists a  $(q + 1, q^{q-1}, 3)$   $q$ -ary code (perfect and MDS).

The case  $t = 2, 3, 4$  is studied in [50], [52], [53], [54], [55] and [75], in the binary linear case (cf. Section 5.6, Proposition 5.7). In terms of density, their results imply:

$$\begin{aligned}\underline{\mu}(2) &\leq 1.424 \\ \underline{\mu}(3) &\leq 1.375 \\ \underline{\mu}(4) &\leq 2.34.\end{aligned}$$

Using nonlinear codes,  $\underline{\mu}(2) \leq 9/8$  is proven in [67] (see also Section 5.1).

We shall now sketch a proof of the Kabatianskii-Panchenko theorem.

The following proposition has been discovered and generalized many times (see [17], [137], [156]). Following [156], we say that a subset  $S$  *t-covers*  $\mathbf{F}_q^n$  using  $A$  if  $A$  is a set of  $N$  vectors of length  $n$ ,  $\{a^1, a^2, \dots, a^N\}$ , of rank  $n$ , such that

$$S + tA = \mathbf{F}_q^n, \tag{3.41}$$

where  $tA := \{x \in \mathbf{F}_q^n; \exists I \subseteq \{1, \dots, N\}, |I| \leq t, \text{ and } x = \sum a^i, i \in I\}$ . In words,  $tA$  is the set of sums of at most  $t$  elements of  $A$ .

With a slight abuse of notation,  $A$  will also denote the  $n \times N$  matrix with column set  $A$ .

**Proposition 3.1** *With  $S$  and  $A$  as just defined, let  $S + tA = \mathbf{F}_q^n$ . Then*

$$C := \{v \in \mathbf{F}_q^N; Av \in S\}$$

*is a code in  $\mathbf{F}_q^N$  with size  $|S|q^{N-n}$  and covering radius at most  $t$ .*

**Proof.**

$$C = \bigcup_{s \in S} \{v; Av = s\}.$$

For any fixed  $s$ , since  $\text{rank}(A) = n$ ,  $|\{v; Av = s\}| = q^{N-n}$ . For the covering radius, observe that  $d(v, C) = i \iff Av \in (S + iA) \setminus (S + (i-1)A)$  and apply (3.41).  $\square$

Another ingredient in the Kabatianskii-Panchenko theorem is the following result, allowing change of the alphabet size without too much change in the density. Let  $R := GF(r)$  and  $Q := GF(q)$  be two alphabets with sizes  $r$  and  $q$ , respectively, and take  $r \leq q$ . Let  $C$  be an  $r$ -ary linear  $[n, k]_1$  code.

**Proposition 3.2** *If  $C$  is a linear  $r$ -ary  $[n, k]_1$  code, then*

$$K_q(n, 1) \leq (q/r)^n |C| \text{ for all } q \geq r.$$

**Proof.** Consider any surjection  $\sigma : Q \longrightarrow R$  that preserves weights, i.e., sends 0 to 0 and nonzero to nonzero. We extend  $\sigma$  in the obvious way to a weight-preserving surjection, also denoted  $\sigma$ , from  $Q^n$  to  $R^n$ .

Since the cosets mod  $C$  partition  $R^n$ —

$$R^n = \bigcup_{x \in L} (x + C),$$

where  $L$  is an appropriate set of coset leaders—we see that  $\{\sigma^{-1}(x + C); x \in L\}$  is a partition  $\pi$  of  $Q^n$ . We now show that each cell of  $\pi$  has covering radius 1.

Let  $u \in Q^n$ , and consider the translate

$$T := u + \sigma^{-1}(x + C).$$

Apply  $\sigma$  to  $T$  to get  $(\sigma(u) + x) + C$ , a coset of  $C$ , with minimum weight 0 or 1 by hypothesis. Since  $\sigma$  preserves weights,  $T$  must also have weight 0 or 1. Picking the smallest  $T$ , say  $T_0$ , we see that  $K_q(n, 1) \leq |T_0| \leq \text{avg } |T|$ .  $\square$

Let us rephrase this result in terms of density. If we start with  $C$  having density  $\mu(C) = |C| \cdot (1 + n(r - 1))r^{-n}$ , then we get a  $q$ -ary code  $C'$  with

$$\frac{\mu(C')}{1 + n(q - 1)} = \frac{|C'|}{q^n} = \frac{|C|}{r^n} = \frac{\mu(C)}{1 + n(r - 1)}.$$

That is,

$$\mu(C') = \mu(C) \cdot \frac{1 + n(q - 1)}{1 + n(r - 1)}.$$

For  $n$  large enough,

$$\mu(C') \simeq \mu(C) \frac{q - 1}{r - 1}. \quad (3.42)$$

3.42, combined with lengthy but direct arguments on the density of powers of prime numbers in the set of integers, allows Kabatianskii and Panchenko to prove:

**Proposition 3.3** [134] *For  $q$  a prime power,  $\mu(q, 1) = 1$ .*  $\square$

In fact, if  $q = rs$ , then Proposition 3.4 gives a stronger result than Proposition 3.2. Though not needed for proving that  $\mu(q, 1) = 1$ , it is of independent interest.

**Proposition 3.4** [17]  $K_{rs}(n, 1) \leq s^{n-1}K_r(n, 1)$ .

**Proof.** Let  $q = rs$ , and let  $Q = \{0, \dots, q-1\}$ ,  $R = \{0, 1, \dots, r-1\}$  and  $S = \{0, 1, \dots, s-1\}$ . Let  $C$  be a covering of  $R^n$  achieving  $K_r(n, 1)$ , not necessarily linear. To every  $z_i \in Q$ , associate the couple  $(x_i, y_i) \in R \times S$  obtained by dividing  $z_i$  by  $s$ :  $z_i = x_i s + y_i := \varphi(x_i, y_i)$ .  $\varphi$  is one-to-one and extends in the obvious way to a mapping  $\varphi : Q^n \longrightarrow R^n \times S^n$ .

Consider the parity-code in  $S^n$  defined by

$$P_S = \{y \in S^n; \sum_{i=1}^n y_i \equiv 0 \pmod{s}\}.$$

**Lemma 3.1**  $P_S$  is an  $\{m_0 = 1, m_1 = 1/n\}$  PWC in  $S^n$  (PWC stands for perfect weighted covering; see [45]).

In other words,  $P_S$  has covering radius 1, and any  $x$  not in  $P_S$  is at distance 1 from  $n$  codewords.

**Proof.** The  $n$  codewords are obtained by fixing  $n - 1$  coordinates in  $x$ .  $\square$

Now define

$$\begin{aligned} C' &= \varphi(C \times P_S) \\ &= \{z \in Q^n; z = \varphi(x, y) \text{ with } x \in C \text{ and } y \in P_S\}. \end{aligned}$$

Let us show that  $C'$  has size  $s^{n-1}|C|$  and covering radius 1. The assertion on the size is obvious. Now take any  $z$  in  $Q^n$ :  $z = (z_1, \dots, z_n) = (\varphi(x_1, y_1), \dots, \varphi(x_n, y_n))$ . Let  $c$  be a word in  $C$  at distance 1 from  $(x_1, \dots, x_n)$ , say  $c = (x_1, x_2, x_{i-1}, c_i \neq x_i, x_{i+1}, \dots, x_n)$ .

Now, by Lemma 3.1, there is a codeword in  $P_S$  differing from  $y$  only on coordinate  $i$ , namely,

$$c' = (y_1, y_2, \dots, y_{i-1}, c'_i = - \sum_{j \neq i} y_j \pmod{s}, y_{i+1}, \dots, y_n).$$

We conclude by noticing that  $\varphi(c \times c')$  is in  $C'$  and differs from  $z$  only on position  $i$ .  $\square$

In terms of density, we get

$$\mu(C') = \frac{r}{q} \mu(C) \frac{1 + n(q-1)}{1 + n(r-1)},$$

and for  $n$  large enough,

$$\mu(C') \simeq \frac{r(q-1)}{q(r-1)} \mu(C),$$

which is better than (3.42) by a factor  $r/q = 1/s$ .

## 4 Upper Bounds for Linear Codes

A linear  $[n, k, d]$  code  $C$  is called:

*Maximal* if for all  $[n, k+1]$  codes  $C'$ ,  $C' \supset C \implies d(C') < d$ ;

*Maximum* if for all  $[n, k+1]$  codes  $C'$ ,  $d(C') < d$ ; in other words,  $k = a[n, d]$ .

*Optimum* if  $n = n[k, d]$ .

*Griesmer* if  $n = g[k, d] \left( := \sum_{0 \leq i \leq k-1} \lceil d \cdot 2^{-i} \rceil \right)$ .

**Theorem 4.1**

$$\begin{array}{cccc} \text{Griesmer} & \implies & \text{Optimum} & \implies & \text{Maximum} & \implies & \text{Maximal} \\ (i) & & (ii) & & (iii) & & (iv) \end{array}$$

**Proof.** (i)  $\implies$  (ii) and (iii)  $\implies$  (iv) are clear. To prove (ii)  $\implies$  (iii), we need to show that there is no  $[n[k, d], k + 1, d]$  code. This will stem from the following:

**Theorem 4.2** *The function  $n[k, d]$  is strictly increasing in  $k$  and  $d$ .*

**Proof.** If there is an  $[n[k + 1, d] = n[k, d], k + 1, d]$  code, shorten it to obtain an impossible  $[n[k, d] - 1, k, d]$  code; to kill the putative  $[n[k, d + 1] = n[k, d], k, d + 1]$  code, puncture it to a contradictory  $[n[k, d] - 1, k, d]$  code.  $\square$

One might think that the better a code for packing, the smaller its covering radius. There is something to that idea:

Define the *deficiency*  $\Delta$  of an  $[n, k, d]$  code by

$$\Delta := a[n, d] - k.$$

Thus  $\Delta = 0$  characterizes maximum codes.

**Proposition 4.1** [77],[264] *An  $[n, k, d]t$  code  $C$  with deficiency  $\Delta$  satisfies*

$$a[t, d] \leq \Delta.$$

**Proof.** Let  $z$  be a coset leader of weight  $t$  (i.e.,  $|z| = d(z, C) = t$ ). We may assume that  $\text{supp}(z) = \{1, 2, \dots, t\}$ . Consider a maximum code  $C'[t, a[t, d], d]$  built on  $\text{supp}(z)$  with generator matrix  $G'$ . If  $G$  is a generator matrix for  $C$ , then the following matrix

$G$	
$G'$	$\underline{0}$

Fig. 1

generates an  $[n, k + a[t, d], d]$  code.  $\square$

The reader should convince himself that he is facing an upper bound on  $t$ , viz,  $t < n[\Delta + 1, d]$ . A nonlinear version of Proposition 4.1 has appeared in [263], namely,

$$\log_2 A(t, d) \leq \log_2 A(n, d) - k.$$

The case  $\Delta = 0$  reads: “Maximum codes have covering radius at most  $d - 1$ .”

Proposition 4.1 can be used to give upper bounds on the covering radius of “worst” codes, i.e., codes with lengths achieving  $s_r(t) - 1$ , which we now define.

Let  $s_r(t) - 1$  denote the maximal length of a code with redundancy  $r$ , minimum distance at least 3 and covering radius greater than  $t$ . In other words, there exists a  $C[s_r(t) - 1, s_r(t) - 1 - r, \geq 3] > t$ , but every code  $C'$  of type  $[s_r(t), s_r(t) - r, \geq 3]$  has  $t(C') \leq t$ .

This parameter is useful when writing on a WOM (write-once memory) (see [40], [49], [209], [264]), using coset coding. The process involves shortening codes with redundancy  $r$  in an arbitrary way. The cost of the writing is the covering radius of the shortened code; thus as long as  $n \geq s_r(t)$ , the cost is at most  $t$ . The following easy result is in [49].

**Proposition 4.2**  $s_r(2) = 2^{r-1} + 1$ . □

A general lower bound is presented in [263], namely

**Proposition 4.3**  $s_r(t) > (t + 2)2^{r-t-1}$ .

**Proof.** Construct a parity-check matrix  $H$  by putting as columns the  $(t + 1)$ -cylinder of  $\mathbb{F}^r$ :  $S = B_1(0^{t+1}) \times \mathbb{F}^{r-(t+1)}$ . In words,  $S$  consists of all the  $r$ -tuples having weight at most 1 on their first  $(t + 1)$  coordinates. Then  $H$  is the parity-check matrix of a  $[(t + 2)2^{r-t-1}, (t + 2)2^{r-t-1} - r]$  code having covering radius  $t + 1$ . □

Zemor conjectures [263] that this lower bound is tight and proves it when  $t = 2^m - 2$ ,  $m \geq 2$ , using Proposition 4.1, which is also used in [264] to derive upper bounds on shortened BCH codes. Let us mention a few of them.

**Proposition 4.4** *Let  $C[n = 2^r - 1, 2^r - 1 - er, 2e + 1]$  be an  $e$ -error-correcting BCH code, and let us shorten it in an arbitrary way to length  $s$ , getting a code  $C(s)$ .*

*For  $e = 2$ :*

*If  $s > (\sqrt{2}/2) n$ , then  $t(C(s)) \leq 7$ .*

*If  $s > (n/2) + n^{1/2}$ , then  $t(C(s)) \leq 9$ .*

*For  $e = 3$ :*

*If  $s > 0.909 n$ , then  $t(C(s)) \leq 12$ .*

*If  $s > 0.722 n$ , then  $t(C(s)) \leq 13$ .*

*If  $s > 0.573 n$ , then  $t(C(s)) \leq 14$ .*

*If  $s > (n/2) + 2n^{1/2}$ , then  $t(C(s)) \leq 16$ .* □

**Definition 4.1** The *residual* of  $C[n, k, d]$  with respect to  $x$ , denoted by  $R(C, x)$ , is the code obtained by projecting  $C$  on the complement of  $\text{supp}(x)$ .

**Proposition 4.5** [243]. *If  $c$  is a codeword of weight at most  $2d - 1$ , then  $R(C, c)$  is an  $[n - |c|, k - 1, d' \geq d - \lfloor |c|/2 \rfloor]$  code.* □

**Remark 4.1** This proposition holds for any acarpous codeword  $c$  (one for which no descendants except  $\emptyset$  are codewords).

Let  $z$  be a coset leader of weight  $t$ . Then for all  $c \in C$

$$t \leq d(z, c) = |z| + |c| - 2|z \cap c|.$$

Hence

$$|c \setminus z| = |c| - |c \cap z| \geq \left\lceil \frac{|c|}{2} \right\rceil.$$

Thus we get

**Theorem 4.3** *If  $z$  is a coset leader of weight  $t$ , then  $R(C, z)$  is an  $[n - t, k, d' \geq \lceil d/2 \rceil]$  code.*  
 $\square$

This new construction of packing codes may be of independent interest. For non-maximal codes ( $t \geq d$ ), and even for codes with  $t = d - 1$ , it outperforms the classical one ( $R(C, c)$ , with  $|c| = d$ ).

Now the existence of  $R(C, z)$  implies

$$n - t \geq g[k, \lceil d/2 \rceil] = g[k, d] + \lceil d \cdot 2^{-k} \rceil - d.$$

This is a new proof of the Janwa bound [129]:

**Corollary 4.1** *For any  $[n, k, d]_t$  code,*

$$t \leq n - g[k, d] + d - \lceil d \cdot 2^{-k} \rceil.$$

$\square$

**Corollary 4.2** [25]. *For a Griesmer  $[n = g[k, d], k, d]_t$  code:*

$$t \leq d - \lceil d \cdot 2^{-k} \rceil.$$

$\square$

Let us derive now an upper bound on  $t$  for maximum codes. First we notice the following obvious characterization:

Let  $C$  be an  $[n, k, d]$  code. Then  $C$  is maximum if and only if  $n < n[k + 1, d]$ .

**Proposition 4.6** [12] *An  $[n, k, d]_t$  maximum code satisfies*

$$t \leq d - (n[k + 1, d] - n).$$

**Proof.** Let  $z$  be a coset leader of weight  $t$ . Suppose indirectly that  $t > d - (n[k + 1, d] - n)$ . Append  $n[k + 1, d] - n - 1$  zeroes to all codewords in  $C$ , getting  $C'$ , and that many ones to  $z$ , getting  $z'$ . The code spanned by  $C'$  and  $z'$  is an impossible  $[n[k + 1, d] - 1, k + 1, d]$ .  $\square$

Define  $b := n[k + 1, d] - n[k, d]$  and note that  $b$  does not depend on a code. Then

**Corollary 4.3** *Optimum  $[n, k, d]_t$  codes satisfy  $t \leq d - b$ .*  $\square$

Notice that if  $n[k, d] = g[k, d]$ , then  $b \geq \lceil d \cdot 2^{-k} \rceil$ . If the inequality is strict, we improve on Corollary 4.2.

**Remark 4.2** We have seen (Theorem 4.2) that  $n[k, d]$  is strictly increasing with  $k$ , i.e.,  $b > 0$ . On the other hand, for all codes  $t \geq \lfloor d/2 \rfloor$ , hence  $b \leq \lceil d/2 \rceil$ , with equality implying that the optimum  $[n, k, d]$  code is perfect or quasi-perfect.

It is easy to check that  $n[2^r - r - 1, 3] = 2^r - 1$  and  $n[2^r - r, 3] = 2^r + 1$ . On the other hand,  $n[12, 7] = 23$ , but  $n[13, 7] = 26$ , achieved by a doubly circulant  $[26, 13, 7]$ , hence

$$n[13, 7] - n[12, 7] < \lceil d/2 \rceil.$$

We summarize this discussion with the final theorem from [12], together with our results on the case of equality.

**Theorem 4.4**  $n[k + 1, d] - n[k, d] \leq \lceil d/2 \rceil$  with equality only when the  $[n[k, d], k, d]$  code is quasi-perfect or is a perfect repetition or Hamming code.  $\square$

Let us sum up the various upper bounds on  $t$ .

**Theorem 4.5** Let  $C$  be an  $[n, k, d]_t$  code with deficiency  $\Delta$ . Then

$$t \leq \min\{n[\Delta + 1, d] - 1, d - \lceil d \cdot 2^{-k} \rceil + n - g[k, d]\}.$$

$$t \leq \begin{cases} d - (n[k + 1, d] - n) & C \text{ maximum} \\ d - b & C \text{ optimum} \\ d - b \leq d - \lceil d \cdot 2^{-k} \rceil & C \text{ Griesmer.} \end{cases}$$

$\square$

Results relating covering radii of code and subcode:

**Proposition 4.7** [124] Let  $C_0$  be a subcode of codimension  $i$  in  $C$ . Denote  $t(C_0)$  by  $R_0$ ,  $t(C)$  by  $R$ . Then

$$2^{R_0} \leq 2^i \sum_{j \leq R} \binom{R_0}{j}.$$

$\square$

This result is an upper bound on  $R_0$  and a lower bound on  $R$ . The proof rests on [141].

Some other such results [132] are more specialized, holding for the even-weight subcode  $C_0$  of a  $t$ -dense code  $C$ . The results are upper bounds on, or exact determinations of,  $t(C)$  in terms of  $t(C_0)$ .

## 5 Improving Upper Bounds by Constructions

If there is an  $[n, k_0]_{t_0}$  code, then it provides upper bounds:  $t[n, k_0] \leq t_0$ , and  $k[n, t_0] \leq k_0$  and analogously for the general case. In this section we discuss several constructions yielding useful upper bounds. We shall mostly deal with *binary* codes, but Section 5.7 will be devoted to *q-ary* and *mixed* codes. It is a remarkable fact that Finnish and Swedish football fans found very good constructions for binary, ternary or mixed binary/ternary codes, including the ternary Golay code in 1947 (see [84], [85] or [111]).

Upper bounds derived in this section will be listed in Tables A, B, and C. Table A gives bounds for  $K(n, t)$  ( $1 \leq n \leq 33, 1 \leq t \leq 10$ ); Table B gives bounds for  $t[n, k]$  ( $1 \leq n \leq 64, 1 \leq k \leq n$ ); Table C gives bounds for  $K_3(n, t)$  ( $1 \leq n \leq 13, 1 \leq t \leq 3$ ).



## 5.1 Direct Sum of Two Codes; Generalization

If  $C_1$  is an  $(n_1, K_1)t_1$  code (resp. an  $[n_1, k_1]t_1$  linear code), and  $C_2$  is an  $(n_2, K_2)t_2$  code (resp. an  $[n_2, k_2]t_2$  linear code), then the *direct sum* (DS) of  $C_1$  and  $C_2$ , denoted by  $C_1 \oplus C_2$ , is  $C_1 \oplus C_2 = \{(u|v); u \in C_1, v \in C_2\}$ . Code  $C_1 \oplus C_2$  is an  $(n_1 + n_2, K_1 K_2)t_1 + t_2$  code (resp. an  $[n_1 + n_2, k_1 + k_2]t_1 + t_2$  linear code). As a consequence, we have the following proposition:

**Proposition 5.1** *For all integers  $n_i \geq t_i \geq 0$  and  $n_i \geq k_i \geq 0$  ( $i = 0, 1, 2$ ),*

$$K(n_1 + n_2, t_1 + t_2) \leq K(n_1, t_1) \cdot K(n_2, t_2); \quad (5.43)$$

$$K(n_0 + 1, t_0) \leq 2K(n_0, t_0); \quad K(n_0 + 1, t_0 + 1) \leq K(n_0, t_0).$$

$$k[n_1 + n_2, t_1 + t_2] \leq k[n_1, t_1] + k[n_2, t_2];$$

$$k[n_0 + 1, t_0] \leq k[n_0, t_0] + 1; \quad k[n_0 + 1, t_0 + 1] \leq k[n_0, t_0].$$

$$t[n_1 + n_2, k_1 + k_2] \leq t[n_1, k_1] + t[n_2, k_2]; \quad (5.44)$$

$$t[n_0 + 1, k_0] \leq t[n_0, k_0] + 1; \quad t[n_0 + 1, k_0 + 1] \leq t[n_0, k_0].$$

□

Using the blockwise direct sum [166, p. 584], [103] and a generalization of norm (see Section 6.3), Struik [236] has produced infinite classes of nonlinear codes with low asymptotic density, e.g.,  $(n, M, 4)2$  codes with  $n = 2^m + 2^{m-1} - 1$  and  $M = 2^{n-2m}$ . The density tends to 9/8 as  $m$  goes to infinity.

## 5.2 Piecewise Constant Codes

Piecewise constant codes can be described in a compact way and sometimes yield good coverings; furthermore, their covering radius is easy to compute. Such a code  $C$  is defined as follows [47]: the length  $n$  of the code is partitioned as  $n = n_1 + n_2 + \dots + n_s$ , and each codeword  $c$  is written according to this partition  $c = (c^{(1)}, c^{(2)}, \dots, c^{(s)})$ , where  $c^{(i)}$  has length  $n_i$ . Now if  $C$  contains one word with  $|c^{(1)}| = w_1, \dots, |c^{(s)}| = w_s$ , then  $C$  contains all such words.

**Example 5.1** The  $(5, 7)1$  code described in Section 6.1, Example 6.1, is a piecewise constant code: the partition is  $5 = 2 + 3$ , and the codewords are

00 000

00 111

10 000

01 000

11 011

11 101

11 110,

which can be described as:  $(0, 0), (0, 3), (1, 0), (2, 2)$ .

$(2t + 3, 7)t, (2t + 4, 12)t$  piecewise constant codes exist for  $t = 1, 2, \dots$

$K(11, 1) \leq 192$  can be proved by combining a piecewise constant code and a Steiner system [47]; the partition is  $11 = 6 + 5$ , and the codewords are: 5 words  $(0, 1)$ , 10 words  $(0, 2)$ , 15 words  $(2, 0)$ , the 66 words of the Steiner system  $S(4, 5, 11)$ , and the complements of all the above 96 words.

### 5.3 Amalgamated Direct Sum for (Sub)Normal Codes

Let  $A$  be an  $(n_A, K_A)t_A$  normal code with last coordinate acceptable, and let  $B$  be an  $(n_B, K_B)t_B$  normal code with first coordinate acceptable; assume that  $A_0^{(n_A)}, A_1^{(n_A)}, B_0^{(1)}, B_1^{(1)}$  are nonempty (see Section 6.1 for definitions and notation). Then the *amalgamated direct sum* (ADS) of  $A$  and  $B$ , denoted  $A \dot{\oplus} B$ , is defined by:

$$A \dot{\oplus} B = \{(a|0|b); (a|0) \in A_0^{(n_A)}, (0|b) \in B_0^{(1)}\} \cup \{(c|1|d); (c|1) \in A_1^{(n_A)}, (1|d) \in B_1^{(1)}\}. \quad (5.45)$$

**Proposition 5.2** [47].  $C = A \dot{\oplus} B$  is a code of length  $n = n_A + n_B - 1$ , containing at most  $K_A \cdot K_B / 2$  codewords, and with covering radius  $t_C$  at most  $t_A + t_B$ .

**Proof.** Let  $z = (x|0|y) \in \mathbb{F}^n$ , with  $x$  arbitrary in  $\mathbb{F}^{n_A-1}$  and  $y$  arbitrary in  $\mathbb{F}^{n_B-1}$ . Then

$$\begin{aligned} 2 \cdot d(z, C) &\leq d(z, C_0^{(n_A)}) + d(z, C_1^{(n_A)}) \\ &\leq d((x|0), A_0^{(n_A)}) + d((x|0), A_1^{(n_A)}) + d((0|y), B_1^{(1)}) + d((0|y), B_0^{(1)}) - 1; \end{aligned}$$

now, using the definition of normality, this leads to  $2 \cdot d(z, C) \leq (2t_A + 1) + (2t_B + 1) - 1 = 2(t_A + t_B) + 1$ .

The same holds for  $z = (x|1|y) \in \mathbb{F}^n$ , which proves that  $t_C \leq t_A + t_B$ .  $\square$

**Remark.** If  $A$  and  $B$  are linear, then  $C$  is linear and has dimension equal to  $\dim(A) + \dim(B) - 1$  [79].

The ADS can be constructed with one normal code and one subnormal code (see Section 6.2): let  $A$  be as above and  $B$  be a subnormal code with same parameters (length, cardinality, covering radius) as above and with acceptable partition  $(B_0, B_1)$ ; assume that  $B_0$  and  $B_1$  are nonempty. Then  $A \dot{\oplus} B$  is defined by

$$A \dot{\oplus} B = \{(a|b); (a|0) \in A_0^{(n_A)}, b \in B_0\} \cup \{(c|d); (c|1) \in A_1^{(n_A)}, d \in B_1\}. \quad (5.46)$$

This code also has covering radius at most  $t_A + t_B$  [102].

**Example 5.2** Amalgamated direct sum of Hamming codes:  $[7, 4]1 \dot{\oplus} [7, 4]1 = [13, 7]2$ , so  $t[13, 7] = 2$ .

Amalgamated direct sum of a Hamming code and a repetition code of odd length: for  $i = 0, 1, \dots, [7, 4]1 \dot{\oplus} [2i + 1, 1]i = [2i + 7, 4]i + 1$ , so for  $n$  odd,  $n \geq 7$ ,  $t[n, 4] = \lfloor (n - 4)/2 \rfloor$  (cf. Section 2.6.2).

Amalgamated direct sum of an  $(n, K)t$  (sub)normal code and a repetition code of odd length: for  $i = 0, 1, \dots, (n, K)t \dot{\oplus} (2i + 1, 2)i = (n + 2i, K)t + i$ , so if  $K(n, t)$  is reached by a (sub)normal code, then  $K(n + 2i, t + i) \leq K(n, t)$  (cf. Section 6.4).

## 5.4 Variation on the $u|u+v$ Construction

If  $C_1$  is an  $(n, K_1)$  code and  $C_2$  is an  $(n, K_2)$  code, then the so-called  $u|u+v$  construction gives a code  $C$  with length  $2n$  and  $K_1 \cdot K_2$  codewords, defined by  $C = \{(u|u+v); u \in C_1, v \in C_2\}$ . Now consider an  $(n, K)1$  code  $C_1$  and let, for  $u \in \mathbf{F}^n$ ,  $\pi(u) = 1$  if  $|u|$  is odd, 0 otherwise.

Let  $C = \{(\pi(u)|u|u+v); u \in \mathbf{F}^n, v \in C_1\}$ . Then ([177] and Katsman, Litsyn, see [47]):

**Proposition 5.3**  $C$  is a  $(2n+1, 2^n K)1$  normal code.  $\square$

**Corollary 5.1**

$$K(2n+1, 1) \leq 2^n \cdot K(n, 1). \quad (5.47)$$

$\square$

**Example 5.3** Let  $C_1$  be an  $(11, 192)1$  code (cf. Example 5.1). Then  $C$  is a  $(23, 3 \cdot 2^{17})1$  code, and  $K(23, 1) \leq 3 \cdot 2^{17}$ .

One way of generalizing this construction is the following [112]. Suppose that  $W$  is a set of  $s$  weights ( $1 \leq s \leq n+2$ ), included in  $\{0, 1, \dots, n+1\}$ :  $W = \{w_1, w_2, \dots, w_s\}$ , with  $w_1 < w_2 < \dots < w_s$  and suppose that an integer  $t (\leq n)$  satisfies

$$w_1 \leq \frac{t+1}{2}; w_s \geq n+1 - \frac{t+1}{2}; \text{ for } k=1, 2, \dots, s-1: w_{k+1} - w_k \leq t+1. \quad (5.48)$$

Denote by  $C_w^{n+1}$  the set of all elements in  $\mathbf{F}^{n+1}$  having weight  $w$ ; let  $C_1 = \bigcup_{w \in W} C_w^{n+1}$ , and  $C_2$  be an  $(n, K)t$  code.

Let  $C = \{(u_0|u|u+v); u_0 \in \mathbf{F}, u \in \mathbf{F}^n, (u_0|u) \in C_1, v \in C_2\}$ .

**Proposition 5.4**  $C$  is a normal  $\left(2n+1, K \cdot \sum_{1 \leq k \leq s} \binom{n+1}{w_k}\right)t$  code.  $\square$

**Example 5.4** The case  $t=1, s=\lfloor \frac{n+1}{2} \rfloor, W=\{0, 2, \dots, 2 \cdot \lfloor \frac{n+1}{2} \rfloor\}$ , with  $C_2$  an  $(n, K)1$  code, shows that Proposition 5.4 is a generalization of Proposition 5.3.

Let  $n=4m-1, t=2m-1$  ( $m \geq 1$ ); the inequalities (5.48) read:  $w_1 \leq m; w_s \geq 3m$ ; for  $k=1, \dots, s-1, w_{k+1}-w_k \leq 2m$ . Choose  $W=\{m, 3m\}$  (in order to minimize  $\sum_{1 \leq k \leq s} \binom{n+1}{w_k}$ ):

now  $|C_1| = 2 \binom{4m}{m}$ . Let  $C_2$  be a repetition code of length  $n$ .

We get a normal  $\left(8m-1, 4 \binom{4m}{m}\right)2m-1$  code, proving that  $K(8m-1, 2m-1) \leq 4 \binom{4m}{m}$ . In particular,  $m=3$  gives  $K(23, 5) \leq 880$ .

In view of Table A, where  $1 \leq n \leq 33$  and  $1 \leq t \leq 10$ , we computed, for  $1 \leq t \leq 10$  and  $1 \leq n \leq 16$ ,  $\min \sum_{1 \leq k \leq s} \binom{n+1}{w_k}$ , with the numbers  $w_i$  satisfying inequalities (5.48). Then, using the best known upper bounds on  $K(n, t)$ , we found the following improvement:

$$K(19, 1) \leq 512 \cdot K(9, 1) \leq 512 \cdot 62 = 31,744 \text{ (instead of } 2^{15} = 32,768 \text{)}.$$

## 5.5 Simulated Annealing

The recently developed simulated annealing algorithms have given several new covering codes, mainly in the binary and ternary cases. The basic idea of these algorithms is as follows: a transition from one state to the next one is always accepted if the function to be minimized decreases in this transition; if the function increases, then the transition is accepted or refused according to some probability, so it is hoped that the algorithm does not get stuck in local minima.

Let us be more explicit: let us assume that you want to construct a binary  $(n, K)t$  code. Take a random  $(n, K)$  code  $C$ . The function  $\sigma(C, n, K, t)$  to minimize is the number of words in  $\mathbf{F}^n$  that are not covered by the code (i.e., are at distance  $> t$  from the code): ideally,  $\sigma(C, n, K, t) = 0$ . A high “temperature”  $T$  is chosen for the code ( $T = n$ , for instance) and then  $T$  is slowly lowered (for instance, by multiplying it by 0.9), until it reaches a fixed threshold ( $T = 0.01n$ , for example), where the algorithm stops (unless it has succeeded before). For each temperature  $T$ , the following subprogram is repeated a fixed number of times (unless it succeeds): randomly change  $C$  into  $C'$  by changing one coordinate of one codeword, and randomly choose a number  $r$  in the interval  $[0, 1]$ . Compute  $\sigma(C', n, K, t)$ . If  $\sigma(C', n, K, t) \leq \sigma(C, n, K, t)$ , then accept the transition from  $C$  to  $C'$ ; if  $\sigma(C', n, K, t) > \sigma(C, n, K, t)$ , then accept this transition only if

$$\exp \left( \frac{\sigma(C, n, K, t) - \sigma(C', n, K, t)}{T} \right) > r. \quad (5.49)$$

So the higher the temperature, the more easily accepted a transition which increases the cost function  $\sigma$ . The algorithm stops either when a code  $C$  has been found for which  $\sigma(C, n, K, t) = 0$ , in which case we have an  $(n, K)t$  code, or when temperature  $T$  has reached its threshold (the code is frozen).

**Example 5.5** In the ternary case, for  $n = 6$ , a record-breaking  $(6, 73)1$  code was found using simulated annealing [145]. The algorithm tried 1000 transitions at each temperature, with an initial temperature equal to 2.0, slowly reduced by a factor 0.995. In the binary case, a  $(9, 62)1$  code was found by simulated annealing [257].

## 5.6 Linear Constructions

The direct sum of two Hamming codes of length  $n_A = 2^r - 1$  (resp.  $n_B = 2^{r+i} - 1, i = 0, 1, \dots$ ), dimension  $k_A = 2^r - r - 1$  (resp.  $k_B = 2^{r+i} - (r + i) - 1$ ) and covering radius 1 yields the

result

$$t[2^{r+i} + 2^r - 2, 2^{r+i} + 2^r - 2r - 2 - i] \leq 2. \quad (5.50)$$

Let  $n_i = 2^{r+i} + 2^r - 2$ : (5.50) now reads  $t[n_i, n_i - (2r + i)] \leq 2$ .

The amalgamated direct sum of the same codes gives

$$t[n_i - 1, n_i - 1 - (2r + i)] \leq 2. \quad (5.51)$$

Actually, when dealing with Hamming codes, it is even possible to improve on ADS, obtaining [79]

$$t[n_i - 2, n_i - 2 - (2r + i)] \leq 2, \quad (5.52)$$

provided  $r = 3$  and  $i \geq 1$ , or  $r \geq 4$ . For  $r$  even, say  $r = 2u$ , we have  $n_0 = 2^{2u+1} - 2$ , and

$$t[n_0 - 2, n_0 - 2 - 4u] \leq 2. \quad (5.53)$$

Now a significant improvement can be brought to (5.53), using projective geometries over large fields:

**Proposition 5.5** [24] For  $u \geq 1$ ,

$$t[n_0 - (2^u - 1), n_0 - (2^u - 1) - 4u] \leq 2. \quad (5.54)$$

□

**Example 5.6**  $r = 4, u = 2$  :  $n_0 = 30$ , and  $t[27, 19] \leq 2$ , whereas (5.53) gives only  $t[28, 20] \leq 2$ .

In the same way, if  $r = 2u$ , (5.52) reads

$$t[n_i - 2, n_i - 2 - (4u + i)] \leq 2, \quad (5.55)$$

and for  $i = 1, 2, 3$ , Proposition 5.6 gives a better result than (5.55):

**Proposition 5.6** [24] For  $u \geq 2, i = 1, 2, 3$ ,

$$t[n_i - (2^{2u+i-1} - 2^{2u} + 2^u), n_i - (2^{2u+i-1} - 2^{2u} + 2^u) - (4u + i)] \leq 2. \quad (5.56)$$

□

**Example 5.7**  $r = 4, u = 2, i = 1$  :  $n_1 = 46$  and  $t[42, 33] \leq 2$ , whereas (5.55) gives only  $t[44, 35] \leq 2$ .

$r = 4, u = 2, i = 2$  :  $n_2 = 78$  and  $t[58, 48] \leq 2$ , whereas (5.55) gives only  $t[76, 66] \leq 2$ . However, in this case it was already proved in [29] that  $t[59, 49] \leq 2$ .

In [50], [52], [53], [54], [55], and [75], other infinite families of linear binary codes can be found; the construction of the parity-check matrices of these codes was explicitly given in [50], [54], [55] and [75], requiring heavy notation, but slightly better results were announced in [52] and [53]. Proposition 5.7 sums up the results thus obtained:

**Proposition 5.7** *There exist linear binary codes with the following parameters:*

$$\begin{aligned}
t = 2 \quad & k = n - 2m, n = 27 \cdot 2^{m-4} - 1, \text{ for } m \geq 4; \\
& k = n - 2m + 1, n = 5 \cdot 2^{m-2} - 1, \text{ for } m \geq 2. \\
t = 3 \quad & k = n - 3m \quad n = 155 \cdot 2^{m-6} - 2, \text{ for } m \geq 6; \\
& \quad \quad \quad n = 76 \cdot 2^{m-5} - 1, \text{ for } m \geq 9; \\
& k = n - 3m + 1 \quad n = 2^{m+1} - 1, \text{ for } m \geq 5; \\
& \quad \quad \quad n = 411 \cdot 2^{m-8} - 2, \text{ for } m \geq 9; \\
& \quad \quad \quad n = 821 \cdot 2^{m-9} - 1, \text{ for } m \geq 14; \\
& k = n - 3m + 2, n = 3 \cdot 2^{m-1} - 1, \text{ for } m \geq 8. \\
t = 4 \quad & k = n - 4m \quad n = 48 \cdot 2^{m-4} - 2, \text{ for } m \geq 6; \\
& \quad \quad \quad n = 47 \cdot 2^{m-4} - 1, \text{ for } m = 5, m \geq 11; \\
& k = n - 4m + 1 \quad n = 11 \cdot 2^{m-2} - 2, \text{ for } m \geq 5; \\
& \quad \quad \quad n = 39 \cdot 2^{m-4} - 3, \text{ for } m \geq 11; \\
& \quad \quad \quad n = 1247 \cdot 2^{m-9} - 1, \text{ for } m = 9, m \geq 16; \\
& k = n - 4m + 2 \quad n = 19 \cdot 2^{m-3} - 2, \text{ for } m \geq 7; \\
& \quad \quad \quad n = 31 \cdot 2^{m-4} - 2, \text{ for } m \geq 9; \\
& \quad \quad \quad n = 31 \cdot 2^{m-4} - 3, \text{ for } m \geq 11; \\
& \quad \quad \quad n = 991 \cdot 2^{m-9} - 1, \text{ for } m \geq 16; \\
& k = n - 4m + 3 \quad n = 2^{m+1} - 2, \text{ for } m \geq 5; \\
& \quad \quad \quad n = 15 \cdot 2^{m-3} - 2, \text{ for } m \geq 7; \\
& \quad \quad \quad n = 14 \cdot 2^{m-3} - 2, \text{ for } m \geq 9; \\
& \quad \quad \quad n = 14 \cdot 2^{m-3} - 3, \text{ for } m \geq 11; \\
& \quad \quad \quad n = 895 \cdot 2^{m-9} - 1, \text{ for } m \geq 16. \quad \square
\end{aligned}$$

**Example 5.8**  $t = 2, k = n - 10$  ( $m = 5$ ),  $n = 27 \cdot 2 - 1$  gives  $t[53, 43] \leq 2$ .

$t = 2, k = n - 9$  ( $m = 5$ ),  $n = 5 \cdot 2^3 - 1 = 39$  gives  $t[39, 30] \leq 2$ .

$t = 3, k = n - 14$  ( $m = 5$ ),  $n = 2^6 - 1 = 63$  gives  $t[63, 49] \leq 3$ .

$t = 4, k = n - 17$  ( $m = 5$ ),  $n = 2^6 - 2 = 62$  gives  $t[62, 45] \leq 4$ .

Some of these constructions can be extended to the  $q$ -ary case (see [50] or [51]).

## 5.7 $q$ -ary and Mixed Codes

We have already mentioned that simulated annealing was used to improve upper bounds on  $K_3(n, t)$ . Other methods borrowed from the binary case can be extended to the  $q$ -ary and mixed case.

For instance, results similar to Proposition 5.1 can be obtained in the  $q$ -ary case as well as in the mixed case (in what follows, we restrict our attention to mixed binary/ternary codes, but the results are easy to extend to general mixed codes; we use the same notation as in Section 2.7): if  $C_1$  (resp.  $C_2$ ) is an  $(n_1, K_1)t_1$  (resp.  $(n_2, K_2)t_2$ ) code included in  $\mathbf{F}_3^T \cdot \mathbf{F}_2^B$ , then the direct sum of  $C_1$  and  $C_2$  is an  $(n_1 + n_2, K_1 \cdot K_2)t_1 + t_2$  code. In particular, letting  $C_1$  be a binary  $(1, 2)0$  or a ternary  $(1, 3)0$  code gives the second part of Proposition 5.8:

**Proposition 5.8** For all integers  $q, T, B, t, n_i \geq t_i$  ( $i = 0, 1, 2$ ),

$$K_q(n_1 + n_2, t_1 + t_2) \leq K_q(n_1, t_1) \cdot K_q(n_2, t_2); \quad (5.57)$$

$$K_q(n_0 + 1, t_0) \leq q \cdot K_q(n_0, t_0); K_q(n_0 + 1, t_0 + 1) \leq K_q(n_0, t_0). \quad (5.58)$$

$$K(T + 1, B, t) \leq 3K(T, B, t). \quad (5.59)$$

□

### 5.7.1 Codes Over $q$ -ary Alphabets

The amalgamated direct sum looks less efficient for  $q > 2$  than in the binary case (see Section 6.2). However, the notions of seminormality and strong seminormality (see Section 6.3) give the following results:

**Proposition 5.9** [191] If  $q$  is a prime power and if  $C$  is a  $q$ -ary  $(n, K)t$  seminormal code, then

$$K_q(n + q, t + 1) \leq q^{q-2} \cdot K. \quad (5.60)$$

□

**Example 5.9**  $q = 3$ ; there exist a  $(6, 73)1$  and a  $(7, 186)1$  seminormal codes. So  $K_3(9, 2) \leq 3 \cdot 73 = 219$ , and  $K_3(10, 2) \leq 3 \cdot 186 = 558$ .

Strongly seminormal codes can be combined efficiently with *any* code: let  $A$  be any  $q$ -ary  $(n_A, K_A)t_A$  code and let  $B$  be a  $q$ -ary  $(n_B, K_B)t_B$  strongly seminormal code, with acceptable partition  $B = \bigcup_{a \in \mathbf{E}_q} B_a$ ; assume that  $A_a^{(n_A)}$  and  $B_a$  are nonempty for all  $a \in \mathbf{E}_q$ , and define  $C = A \dot{\oplus} B = \bigcup_{a \in \mathbf{E}_q} \{(c|d); (c|a) \in A_a^{(n_A)}, d \in B_a\}$ . Then, as usual,  $C$  is an

$(n_A + n_B - 1, K \leq K_A \cdot K_B/q)t \leq t_A + t_B$  code [191].

**Example 5.10**  $q = 3$ ; there exists a ternary strongly seminormal  $(6, 18)2$  code. So  $K_3(n + 5, t + 2) \leq 6K_3(n, t)$ : for  $n = 4, t = 1$ , this leads to  $K_3(9, 3) \leq 54$ .

Various generalizations of the  $u|u + v$  construction (cf. Section 5.4) have been published. Let us begin with an example.

**Example 5.11** Let  $C_1$  be a ternary  $(4, 9)1$  Hamming code. Let

$$C = \left\{ (u_0|u|u + v); u \in \mathbf{F}_3^4, v \in C_1, u_0 \in \mathbf{F}_3, u_0 \neq \sum_{1 \leq i \leq 4} u_i \right\}.$$

Then  $C$  is a  $(9, 2 \cdot 3^4 \cdot 9 = 1458)1$  code [137].

This construction was generalized to any  $q$ -ary  $(n, K)_1$  code  $C_1$  in the following way [156]. Let  $\mathbf{E}_q$  stand for  $\mathbf{F}_q$  or for the ring of integers mod  $q$  and let

$$C = \left\{ (u_0 | u | u + v); u \in \mathbf{E}_q^n, v \in C_1, u_0 \in \mathbf{E}_q, u_0 \neq \sum_{1 \leq i \leq n} u_i \right\}.$$

**Proposition 5.10**  *$C$  is a  $(2n + 1, (q - 1) \cdot q^n \cdot K)_1$  normal code.* □

**Corollary 5.2** *For all  $q \geq 2$ ,*

$$K_q(2n + 1, 1) \leq (q - 1) \cdot q^n \cdot K_q(n, 1). \quad (5.61)$$

□

Other similar constructions [17], [105], [156], lead to the following results:

**Proposition 5.11**

$$\text{If } q \text{ is a prime, } K_q(qn + 1, 1) \leq q^{n(q-1)} \cdot K_q(n, 1). \quad (5.62)$$

$$\text{If } q \text{ is a prime power, } K_q(qn + 1, t) \leq q^{n(q-1)} \cdot K_q(n, t). \quad (5.63)$$

$$\text{If } q \text{ is a prime and } 1 \leq p \leq q, K_q(pn + 1, t) \leq s \cdot q^{n(p-1)} \cdot K_q(n, t), \quad (5.64)$$

where  $s = \max\{1, q - (p - 1)t\}$ .

□

Inequality (5.63) generalizes inequality (5.62) to any  $t$ .

For  $q$  prime,  $p = 2$  and  $t = 1$ , (5.64) reads:  $K_q(2n + 1, 1) \leq (q - 1) \cdot q^n \cdot K_q(n, 1)$ ; and for  $p = q$  and  $t \geq 1$ , it reads:  $K_q(qn + 1, t) \leq q^{n(q-1)} \cdot K_q(n, t)$ .

So (5.64) generalizes Corollary 5.2 and (5.63) (but only for  $q$ , a prime number).

**Example 5.12**  $q = 3, n = 3$ : (5.62) reads  $K_3(10, 1) \leq 3^6 \cdot K_3(3, 1) \leq 3^6 \cdot 5 = 3645$ .

Table C gives bounds for  $K_3(n, t)$  ( $1 \leq n \leq 13, 1 \leq t \leq 3$ ). Tables of upper bounds for  $K_3(n, t)$  ( $1 \leq n \leq 14, 1 \leq t \leq 9$ ),  $K_4(n, t)$  ( $1 \leq n \leq 10, 1 \leq t \leq 7$ ) and  $K_5(n, t)$  ( $1 \leq n \leq 9, 1 \leq t \leq 7$ ) appeared in [191].

### 5.7.2 Codes Over Mixed Alphabets

Again we restrict our attention to the case of binary/ternary codes; some general simple constructions can be used, giving the following upper bounds:



**Proposition 5.12** [85]  $\forall T, B, t \in \mathbb{N}$ ,

$$K(T+1, B, t) \leq \frac{3}{2}K(T, B+1, t); \quad (5.65)$$

$$K(T, B+1, t) \leq K(T+1, B, t); \quad (5.66)$$

$$K(T, B+3, t) \leq \frac{8}{3}K(T+1, B, t); \quad (5.67)$$

$$K(T+4, B, t+1) \leq 3K(T, B+2, t). \quad (5.68)$$

□

Other results, using piecewise constant codes, the Steiner system  $S(4, 5, 11)$  (cf. Section 5.2), or various ad hoc methods, can be found in [85], where a table of upper bounds for mixed binary/ternary codes (for  $n = T + B \leq 13$  and  $t \leq 3$ ) is given; of course, this table also provides results for binary and ternary codes (i.e.,  $T = 0$  or  $B = 0$ ), see Tables A and C. There is a more recent table (with the same parameters) in [199], and a new one will appear in [200].

Finally, let us mention that mixed codes can be used to construct good binary covering codes (see, for instance, [67], [190] or [192]—cf. Section 9.1).

## 6 Normality

### 6.1 Basic Definitions and Properties

The notion of *normality* was first introduced for linear binary codes in [79], then for all binary codes in [47].

**Definition 6.1** Let  $C$  be a binary code, linear or nonlinear, with length  $n$  and covering radius  $t$ . For  $i = 1, 2, \dots, n$ , and  $a = 0$  or  $1$ , let  $C_a^{(i)}$  denote the subset of codewords of  $C$  with  $i^{\text{th}}$  coordinate equal to  $a$ ; for any vector  $x$  in  $\mathbf{F}^n$ , let

$$N^{(i)} = \max_{x \in \mathbf{F}^n} \left\{ d(x, C_0^{(i)}) + d(x, C_1^{(i)}) \right\} \quad (6.69)$$

be the *norm of  $C$  with respect to coordinate  $i$* , with the convention that  $d(x, \emptyset) = n$ . Any number  $N$  satisfying

$$N^{(i)} \leq N, \quad (6.70)$$

for at least one  $i$ , is a *norm* for code  $C$ , and any coordinate  $i$  for which (6.70) holds is called *acceptable with respect to  $N$* .

Code  $C$  is said to be *normal* if it has norm  $N$  satisfying

$$N \leq 2t + 1, \quad (6.71)$$

and any coordinate  $i$  such that  $N^{(i)} \leq 2t + 1$  is called *acceptable* (so acceptable will mean acceptable with respect to  $2t + 1$ ).

In other words, code  $C$  is normal if there exists a coordinate  $i$ , called acceptable, such that  $\forall x \in \mathbf{F}^n, d(x, C_0^{(i)}) + d(x, C_1^{(i)}) \leq 2t + 1$ .

**Example 6.1**  $K(5,1)=7$  is attained by the following  $(5,7)1$  code:  $C = \{00000, 00111, 10000, 01000, 11011, 11101, 11110\}$  (cf. Section 5.2, Example 5.1). For  $i = 1, \dots, 5, N^{(i)} = 3$ ;  $C$  has norm 3,  $C$  is normal, and every coordinate is acceptable.

Normality is an interesting notion because normal codes have two nice properties:

- It seems that a lot of binary codes, in particular the linear codes, are normal (see Propositions 6.2—6.12 below). Actually, no abnormal linear code is known, and very few abnormal nonlinear codes have been exhibited (cf. Proposition 6.1 below).
- Two normal codes can efficiently be combined, in a so-called *amalgamated direct sum* (ADS): if  $C_1$  is an  $(n_1, K_1)t_1$  code (resp. an  $[n_1, k_1]t_1$  linear code), and  $C_2$  is an  $(n_2, K_2)t_2$  code (resp. an  $[n_2, k_2]t_2$  linear code), then it is possible to construct an  $(n_1 + n_2 - 1, K \leq K_1 \cdot K_2/2) t \leq t_1 + t_2$  code (resp. an  $[n_1 + n_2 - 1, k_1 + k_2 - 1]t \leq t_1 + t_2$  linear code), which we shall denote  $C_1 \dot{\oplus} C_2$ . See Proposition 5.2 for more detail. Compared to the *direct sum* (DS) of  $C_1$  and  $C_2$ ,  $C_1 \oplus C_2$ , (cf. Proposition 5.1), we get a length decreased by 1, a cardinality divided by 2 (or a dimension decreased by 1), and the same covering radius; so from a covering viewpoint, for normal codes ADS is always at least as efficient as DS.

The complexity of computing the smallest norm of a code, or determining whether a code is normal or not, is not known. These problems, stated as decision problems, read:

NAME: Norm of a code.

INSTANCE: A binary code  $C$  of length  $n$ , an integer  $w$ .

QUESTION: Is there an  $i$  ( $1 \leq i \leq n$ ) such that:

$$\forall x \in \mathbf{F}^n, d(x, C_0^{(i)}) + d(x, C_1^{(i)}) \leq w?$$

NAME: Normality of a code.

INSTANCE: A binary code  $C$  of length  $n$ .

QUESTION: Is there an  $i$  ( $1 \leq i \leq n$ ) such that:

$$\forall x \in \mathbf{F}^n, d(x, C_0^{(i)}) + d(x, C_1^{(i)}) \leq 2t + 1,$$

where  $t$  is the covering radius of  $C$ ?

We recall that the problem of computing the covering radius of a binary *linear* code is  $\Pi_2$ -complete [175]. A very recent result is that computing the covering radius of a binary code is NP-complete [74]. The seemingly paradoxical fact that the linear case might be harder than the general unrestricted case is due to the more compact representation of linear codes.

We shall now describe the first code that was shown to be abnormal by P. Frankl in [139, II]; since then, other abnormal codes were found (see [251], where abnormal codes, with arbitrary covering radius, are given, or [113], showing an abnormal  $(9,118)1$  code, which is, to our knowledge, the smallest abnormal code with covering radius 1, cf. Proposition 6.12).

Let  $B$  be a code of length  $n$  and minimum distance  $d \geq 6$ , containing at least  $n$  codewords. Let  $b^{(1)}, b^{(2)}, \dots, b^{(n)}$  be  $n$  distinct codewords for which we assume, without loss of generality, that the  $i^{\text{th}}$  coordinate of  $b^{(i)}$  is equal to 0. Let  $S_i$  be the sphere of radius  $\lfloor (d-2)/2 \rfloor$ , centered at  $b^{(i)}$ , restricted to vectors with  $i^{\text{th}}$  coordinate equal to 0. Let  $C = \mathbf{F}^n \setminus (S_1 \cup S_2 \cup \dots \cup S_n)$ .

**Proposition 6.1**  *$C$  is abnormal.*

**Proof.** If  $z$  is not a codeword, then  $z$  belongs to a unique  $S_i$ , because, by the triangle inequality, the  $S_i$  are disjoint; let  $c$  be obtained from  $z$  by changing its  $i^{\text{th}}$  coordinate to 1. Then  $d(c, z) = 1$ ,  $c \notin S_i$ , and  $d(c, b^{(i)}) \leq \lfloor d/2 \rfloor$ ; therefore, for all  $j \neq i$ ,  $d(c, b^{(j)}) \geq \lfloor d/2 \rfloor$ , so  $c \notin S_j$ , and  $c$  belongs to  $C$ . This proves that  $C$  has covering radius  $t = 1$ .

For all  $i$ ,  $d(b^{(i)}, C_0^{(i)}) \geq \lfloor d/2 \rfloor$ ,  $d(b^{(i)}, C_1^{(i)}) \geq 1$ , so  $C$  has norm at least  $\lfloor d/2 \rfloor + 1 \geq 4 = 2t + 2$ : no coordinate is acceptable, and  $C$  is not normal.  $\square$

**Example 6.2** Based on this idea, in [139, II] an abnormal (11,1432)1 code was built, then an abnormal (10,564)1 code, and, by omitting many of these 564 codewords, an abnormal (10,217)1 code. These codes, as well as the abnormal (9,118)1 code mentioned above, are bad covering codes, since  $55 \leq K(9, 1) \leq 62$ ,  $105 \leq K(10, 1) \leq 120$ ,  $177 \leq K(11, 1) \leq 192$  (see Table A).

On the other hand, large classes of binary codes are normal; the following propositions gather the main results we know:

**Proposition 6.2** [79] *The following binary linear codes are normal:  $\mathbf{F}^n$ ; the repetition code  $\{0^n, 1^n\}$ ; the code consisting of all vectors of length  $n$  and even weight; Hamming codes; extended Hamming codes; the perfect and extended perfect Golay codes of lengths 23 and 24; perfect codes; the direct sum of two normal linear codes; all simplex codes; the first-order Reed-Muller codes of length  $n = 2^m$ , for  $m = 3, m = 5$  or  $m$  even.*  $\square$

A recent result:

**Proposition 6.3** [127] *The first-order Reed-Muller code of length  $2^7$  is normal.*  $\square$

**Proposition 6.4** [114] *Let  $m$  be the order of 2 modulo  $n$  and  $N$  a divisor of  $2^m - 1$ ; the binary narrow-sense BCH codes of length  $n = (2^m - 1)/N$  are normal for all large  $m$ .*  $\square$

**Proposition 6.5** [139, II] *The following binary linear codes are normal: codes with length  $\leq 14$ ; codes with dimension  $\leq 5$ .*  $\square$

**Proposition 6.6** [120] *The following binary linear codes are normal: codes with minimum distance  $\leq 4$ ; codes with covering radius  $\leq 3$ .*  $\square$

Actually, it was stated earlier that any binary linear code with minimum distance  $\leq 5$  is normal, but this result remains to be proved, as was pointed out in [120].

**Proposition 6.7** [133] *Each binary  $[n, k]$  code with  $n - k \leq 7$  or  $n = 15$  is normal.*  $\square$

**Proposition 6.8** [123] *Any perfect or quasi-perfect binary linear code is normal.*  $\square$

Results in the nonlinear case also exist; the following result was proved independently in [113] and [251]:

**Proposition 6.9** *Any binary code of length  $n$ , with covering radius 1, and containing  $K(n, 1)$  codewords (i.e., any optimal code with covering radius 1) is normal.*  $\square$

**Proposition 6.10** [251] *Any binary code with covering radius  $t$  and minimum distance  $\geq 2t$  is normal.*  $\square$

**Proposition 6.11** [68] *Any binary code with covering radius  $t$  and minimum distance  $2t - 1$  is normal if  $t$  does not divide  $n$ .*  $\square$

Propositions 6.8, 6.10, and 6.11 strengthen the result in Proposition 6.2 about perfect codes. On the other hand, there exist abnormal codes with covering radius  $t = 2$ , minimum distance  $d = 3 (= 2t - 1)$ , and length  $2^n$  (divisible by 2) [68].

**Proposition 6.12** [113] *The following binary codes are normal: codes with covering radius 1 and length  $\leq 8$ ; codes with covering radius 1 and cardinality  $\leq 95$ ; codes with length  $n$ , covering radius 1 and cardinality  $\leq K(n, 1) + n - 1$ .*  $\square$

The last statement of Proposition 6.12 improves Proposition 6.9.

## 6.2 Subnormality

**Definition 6.2** [99] Let  $C$  be a binary code, linear or nonlinear, with length  $n$  and covering radius  $t$ . Let  $C_0$  be a subset of  $C$ , and  $C_1 = C \setminus C_0$ .  $C$  is said to be *subnormal with respect to  $(C_0, C_1)$* , and  $(C_0, C_1)$  is called an *acceptable partition* of  $C$ , if

$$\max_{x \in \mathbf{F}^n} \{d(C_0, x) + d(C_1, x)\} \leq 2t + 1, \quad (6.72)$$

with the convention that  $d(x, \emptyset) = n$ .

Code  $C$  is *subnormal* if at least one acceptable partition exists.

In other words, code  $C$  is subnormal if there exists a partition  $(C_0, C_1)$  of  $C$  such that  $\forall x \in \mathbf{F}^n, d(C_0, x) + d(C_1, x) \leq 2t + 1$ .

Subnormal codes have the following advantages:

- They are more numerous than normal codes, for any normal code is subnormal, with the partition  $(C_0^{(i)}, C_1^{(i)})$  acceptable; this inclusion is strict, since it is known that all codes with covering radius 1 are subnormal [104], which shows that the abnormal code of Proposition 6.1 is subnormal. Actually, there is no known example of a code that is not subnormal.

- The ADS can be constructed with one normal code and one subnormal code, instead of two normal codes, and still give the same parameters [102]. However, we do not know of a case where this has led to an improvement on  $K(n, t)$  (or  $k[n, t]$ ).

Before closing Section 6.2, let us mention that the notions of normality and subnormality can be very easily extended to the  $q$ -ary case by replacing (6.69), (6.71), and (6.72), respectively, by

$$N^{(i)} = \max_{x \in \mathbf{E}_q^n} \left\{ \sum_{a \in \mathbf{E}_q} d(x, C_a^{(i)}) \right\} \quad (6.73)$$

$$N \leq qt + q - 1; \quad (6.74)$$

$$\max_{x \in \mathbf{E}_q^n} \left\{ \sum_{0 \leq i \leq q-1} d(C_i, x) \right\} \leq qt + q - 1. \quad (6.75)$$

Now the ADS of two normal  $q$ -ary codes, or of a normal  $q$ -ary code and a subnormal  $q$ -ary code,  $C_1$  (length  $n_1$ ,  $K_1$  elements, covering radius  $t_1$ ) and  $C_2$  (length  $n_2$ ,  $K_2$  elements, covering radius  $t_2$ ), gives a code with length  $n_1 + n_2 - 1$ , cardinality  $K \leq K_1 \cdot K_2 / q$ , covering radius  $t \leq t_1 + t_2$  [163].

Unfortunately, in the case  $q > 2$ , unlike in the case  $q = 2$ , we could not for the moment take advantage of the ADS, since good covering codes are often abnormal and not even subnormal.<sup>1</sup> For instance, we have the following result, which is to be compared to Propositions 6.8, 6.10, or 6.11:

**Proposition 6.13** [163] *No nonbinary nontrivial perfect code is subnormal.* □

### 6.3 Seminormality and Other Definitions

We define *seminormal* and *strongly seminormal* in the  $q$ -ary case, since it is for  $q > 2$  that these notions look better adapted than the notions of normality and subnormality.

**Definition 6.3** [191] A  $q$ -ary  $(n, K)t$  code  $C$  is *seminormal* if there is a partition of  $C$  into  $q$  subsets  $C_a$  ( $a \in \mathbf{E}_q$ ) such that, for all  $x \in \mathbf{E}_q^n$  with  $d(x, C) = t$ ,

$$\max_{a \in \mathbf{E}_q} \{d(x, C_a)\} \leq t + 1. \quad (6.76)$$

$C$  is *strongly seminormal* if (6.76) holds for all  $x \in \mathbf{E}_q^n$ . In both cases, a partition such that (6.76) is satisfied is called *acceptable*.

In general, neither of the sets of seminormal and subnormal codes is a subset of the other one. But in the binary case, all subnormal codes are seminormal. Strongly seminormal codes form a proper subset of seminormal codes.

---

<sup>1</sup>We beseech our colleagues to write “not subnormal” instead of the absurd neologism “absubnormal.”

The interest in these definitions is that constructions similar to ADS can be used with seminormal and strongly seminormal codes (see Section 5.7.1).

Struik [236] proposes a more general definition of normality: Let  $C \subset \mathbb{F}^n$ , of covering radius  $t$ , be the union of two disjoint subsets  $C_0$  and  $C_1$ . Suppose that the norm of  $C$  with respect to  $(C_0, C_1)$ , as he defines it, namely,

$$N = \max_{x \in \mathbb{F}^n} \{d(x, C_0) + d(x, C_1)\},$$

satisfies  $N \leq 2t + 1$ . Then (as in (6.72)) he calls  $C$  *subnormal* with respect to  $(C_0, C_1)$ . The coordinate  $i$  is *suitable* if  $C$  punctured at  $i$  has norm less than  $N$  (with respect to  $C_0$  and  $C_1$  punctured at  $i$ ). If both conditions hold he calls  $C$  *normal*. He points out that normality as defined in (6.71) is, in his terms, subnormality with respect to subsets  $C_0^{(i)}$  and  $C_1^{(i)}$  for some coordinate  $i$ .

Other concepts of normality have been introduced; for the sake of simplicity, we content ourselves with referring the reader to [191] for  $p$ -seminormality,  $p$ -subnormality, [103] for  $(a, b)$ -subnormality and [193] for  $(a, b)$ -normality. It seems that the last word on normality has yet to be written.

## 6.4 The Conjecture $K(n + 2, t + 1) \leq K(n, t)$

A special case of ADS consists of combining a subnormal  $(n, K)t$  code with the repetition code  $\{000, 111\}$ , which has covering radius 1 and is normal. This gives an  $(n + 2, K)t + 1$  code (the linear case gives an  $[n + 2, k]t + 1$  code from an  $[n, k]t$  subnormal code).

So normality and subnormality are directly connected with the following conjectures, which were first stated in [43] (Conjecture 6.1) and [47] (Conjectures 6.2 and 6.3):

**Conjecture 6.1** For  $k \geq 1$ ,

$$t[n + 2, k] \leq t[n, k] + 1. \quad (6.77)$$

**Conjecture 6.2** For  $n \neq t$ ,

$$k[n + 2, t + 1] \leq k[n, t]. \quad (6.78)$$

**Conjecture 6.3** For  $n \neq t$ ,

$$K(n + 2, t + 1) \leq K(n, t). \quad (6.79)$$

**Theorem 6.1** *Conjectures 6.1 and 6.2 are equivalent.*

**Proof.** Assume that for  $n \neq t$ ,  $k[n + 2, t + 1] \leq k[n, t]$ , and that there exist  $n_0$  and  $k_0 \geq 1$  such that  $t[n_0 + 2, k_0] > t[n_0, k_0] + 1$ . Set  $t_0 = t[n_0, k_0]$ . Then  $k[n_0, t_0] \leq k_0$  and  $k[n_0 + 2, t_0 + 1] > k_0$  and, therefore,  $k[n_0 + 2, t_0 + 1] > k[n_0, t_0]$ , which is possible only if  $n_0 = t_0$ . But in this case,  $k[n_0 + 2, t_0 + 1] = 1 > k_0$ , contradicting  $k_0 \geq 1$ .

Assume that for  $k \geq 1$ ,  $t[n + 2, k] \leq t[n, k] + 1$ , and that there exist  $n_0$  and  $t_0$  ( $n_0 \neq t_0$ ) such that  $k[n_0 + 2, t_0 + 1] > k[n_0, t_0]$ . Set  $k_0 = k[n_0, t_0]$  and  $k[n_0 + 2, t_0 + 1] = k_0 + l_0$  ( $l_0 > 0$ ). Then  $t[n_0 + 2, k_0] \geq t[n_0 + 2, k_0 + l_0 - 1] > t_0 + 1$  and  $t[n_0, k_0] \leq t_0$  and, therefore,

$t[n_0, k_0] + 1 < t[n_0 + 2, k_0]$ , which is possible only if  $k_0 = 0$ . But in this case,  $t_0 > n_0$ , thus  $t_0 + 1 \geq n_0 + 2$ , and  $k[n_0 + 2, t_0 + 1] = 0$ , contradicting  $k[n_0 + 2, t_0 + 1] > k[n_0, t_0]$ .  $\square$

Conjecture 6.1 was based on the fact that it holds for  $n$  large enough with respect to  $n - k$  or  $k$  [139, I]. The same kind of result, proved by using shortened Hamming codes, supports Conjecture 6.3:

**Proposition 6.14** [47] *For all  $t$  there exists an  $n_0 = n_0(t)$  such that  $K(n+2, t+1) \leq K(n, t)$  for all  $n \geq n_0$ .*  $\square$

Conjecture 6.3 has been proved to be true in the case  $t = 1$ , by various ways we shall shortly describe. Before doing that, however, let us mention that for  $t = 2$ , the smallest unsettled case is for  $n = 8$ : we know only that  $K(8, 2) \geq 11$  and  $K(10, 3) \leq 12$ ; but for  $n \geq 379$ ,  $K(n+2, 3) \leq K(n, 2)$  holds.

In [48] the proof of Proposition 6.14 and the study of small values of  $n$  showed that Conjecture 6.3 was true (for  $t = 1$ ) for all  $n > 1$ , except possibly  $n = 9$  and  $n = 16$ .

The result  $K(16, 1) = 4096$  [250] (instead of  $3933 \leq K(16, 1) \leq 4096$  previously known), together with  $K(18, 2) \leq 4096$  (which was also improved [199], down to 3040) ruled out the case  $n = 16$ . The result  $K(11, 2) \leq 44$  [85] (instead of 56), together with  $K(9, 1) \geq 54$  (now improved [80] to 55), completed the proof in the case  $t = 1$ .

Let us now consider Conjectures 6.4 (stated in [47]) and 6.5:

**Conjecture 6.4** Among the optimal covering codes (i.e., those attaining  $K(n, t)$  or  $t[n, k]$ ) there exists at least one normal code.

**Conjecture 6.5** Among the optimal covering codes there exists at least one subnormal code.

Obviously, Conjecture 6.4 implies Conjecture 6.5, which implies Conjectures 6.1, 6.2, and 6.3. Now Proposition 6.9, or the last part of Proposition 6.12, or the subnormality of any code with covering radius 1 [104], mentioned in Section 6.2, both prove Conjecture 6.3 for  $t = 1$ .

Results on normality given in Section 6.1 also give cases where Conjectures 6.1, 6.2, or 6.3 hold.

## 7 Specific Classes of Codes

### 7.1 Covering Radius of Reed-Muller Codes

Reed-Muller (RM) codes are among the most interesting families in the study of covering radius.

Let  $\rho(r, m)$  be the covering radius of the RM code  $R(r, m)$  of length  $n = 2^m$ , order  $r$ , minimum distance  $d = 2^{m-r}$  and number of information symbols  $k = \sum_{i=0}^r \binom{m}{i}$ . RM codes of the same length constitute a nested family, i.e.,  $R(1, m) \subset R(2, m) \subset \dots \subset R(m, m)$ .

The following exact results are known.

$$\begin{aligned}\rho(m, m) &= 0, \\ \rho(m-1, m) &= 1, \\ \rho(m-2, m) &= 2, \\ \rho(m-3, m) &= \begin{cases} m+2, & m \text{ even}, \\ m+1, & m \text{ odd}, \end{cases} \quad [174] \\ \rho(1, m) &= 2^{m-1} - 2^{(m-2)/2}, m \text{ even} \quad [212].\end{aligned}$$

The following lemma is very helpful (see [214], [44]).

**Lemma 7.1**  $2\rho(r, m-1) \leq \rho(r, m) \leq \rho(r-1, m-1) + \rho(r, m-1)$ .

**Proof.** Use the inductive definition of RM codes. □

More recently Hou has proved

**Proposition 7.1** [126] For  $0 \leq r \leq m-2$ ,  $\rho(r+1, m+2) \geq 2\rho(r, m) + 2$ . □

Using Lemma 7.1 along with the sphere-covering bound, it was shown in [44] that, in spite of being weak error-correcting codes, RM codes are asymptotically good coverings, at least for small values of  $(m-r)$ .

We use the notation  $\lesssim$  as follows:  $f(x) \lesssim g(x)$  iff  $f(x) = g(x)(1 + o(1))$ .

**Proposition 7.2** For  $m$  large enough:

If  $3 \leq m-r = o(m)$ , then

$$\frac{m^{m-r-2}}{(m-r-1)!} \lesssim \rho(r, m) \lesssim \frac{m^{m-r-2}}{(m-r-2)!};$$

if  $2 \leq r = o(m)$ , then

$$2^{m-1} - 2^{m/2} m^{r/2} ((\log_e 2)/2r!)^{1/2} \lesssim \rho(r, m) \lesssim 2^{m-1} - 2^{(m-2)/2} (\sqrt{2} + 1)^{r-1};$$

if  $r/m = \text{const}$ ,  $r/m > 1/2$ , then

$$(2m^3)^{-1/2} 2^{mH(r/m)} \lesssim \rho(r, m) \lesssim 2^{mH(r/m)};$$

if  $r/m = \text{const}$ ,  $(2 + \sqrt{2})^{-1} \leq r/m < 1/2$ , then

$$2^{m-1} - ((\log_e 2)/2)^{1/2} 2^{m(1+H(r/m))/2} \lesssim \rho(r, m) \lesssim 2^{m-1} - 2^{mH(r/m)};$$

if  $r/m = \text{const}$ ,  $0 \leq r/m \leq (2 + \sqrt{2})^{-1}$ , then

$$2^{m-1} - ((\log_e 2)/2)^{1/2} 2^{m(1+H(r/m))/2} \lesssim \rho(r, m) \lesssim 2^{m-1} - (\sqrt{2} + 1)^{r-1} 2^{(m-2)/2};$$

if  $r/m = 1/2$ , then

$$n/4 \gtrsim \rho(m/2, m) \gtrsim nH^{-1}(1/2) \approx 0.11n,$$

i.e.,  $\rho(m/2, m) = \Theta(n)$ . □



The last case is due to the Delsarte bound (see [242]).

The most puzzling case is  $\rho(1, m)$  for odd  $m$ . In [93] the following inequality was proved:

$$2^{m-1} - 2^{(m-1)/2} \leq \rho(1, m) < 2^{m-1} - 2^{(m-2)/2}. \quad (7.80)$$

For  $m = 15$ , a coset at distance larger than the lower bound of (7.80) was discovered in [203], [204]. Using that bound and Lemma 7.1 we get

$$2^{m-1} - \frac{27}{32} 2^{(m-1)/2} \leq \rho(1, m), \text{ for } m \text{ odd, } m \geq 15.$$

For short lengths ( $m = 5, 7$ ) the lower bound of (7.80) is known to be tight. It was shown in [9] for  $m = 5$ , and [185] for  $m = 7$ . The key technique is based on the equivalence of the considered problem with the existence of self-complementary codes without repeated coordinates ( $d^\perp \geq 3$ ). For example, the proof in [185] reduces to demonstrating the non-existence of a  $[57, 8, 25]$  self-complementary code.

The following two conjectures about  $\rho(1, m)$  were stated in [203] and [19].

**Conjecture 7.1** The upper bound in (7.80) is asymptotically tight, i.e.,

$$\lim_{m \rightarrow \infty} \frac{2^{m-1} - \rho(1, m)}{2^{(m-2)/2}} = 1.$$

**Conjecture 7.2** For  $m \geq 3$ ,  $\rho(1, m)$  is even.

The first unknown case is whether  $\rho(1, 9) = 240$ . Langevin [150] showed that if some vector is at distance more than 240 from  $R(1, 9)$ , then it does not belong to  $R(3, 9)$ .

Several topics are related to the study of  $\rho(1, m)$ . The complete weight distribution of the cosets of  $R(1, 4)$ ,  $R(1, 5)$ , and  $R(1, 6)$  can be found in [222], [9], and [167].

In these papers the symmetry group of  $R(1, m)$  is exploited to partition cosets into equivalence classes. This approach to deriving the coset weight distribution is not promising for larger  $m$ . The number of cosets with minimum weight up to  $2^{m-2} + 2^{m-4}$  was determined in [66].

The structure of cosets of  $R(1, m)$  was considered in [20], [19], [150]. An *urcoset* [94], or *orphan* [20], is defined as a coset that is not a descendant. In [20], [19] the urcosets of  $R(1, m)$  have been characterized. For  $m \leq 5$ , all orphans of  $R(1, m)$  are identified.

The cosets of the simplex code were studied in [94].

Normality of  $R(1, m)$  was conjectured in [79]. The conjecture was proved for  $m$  even and for  $m = 3, 5$ , and  $7$  (cf. Propositions 6.2 and 6.3). For a non-computer proof for  $m = 5$ , see [125].

Particular values of  $\rho(r, m)$  for  $r > 1$  were also extensively studied. Bounds were mainly based on the use of Lemma 7.1 with known exact values of  $\rho(r, m)$ . We'll mention the following results for lengths up to 128:

$\rho(2, 6) = 18$  [214] (explicit construction of the coset leader along with the upper bound of Lemma 7.1);

$40 \leq \rho(2, 7) \leq 44$  ([125] for the lower bound, [126] for the upper bound);  
 $20 \leq \rho(3, 7) \leq 23$  (explicit construction of a coset for the lower bound, the Delsarte bound [58] for the upper. See [125]).

For other bounds exploiting relations between the dual distance of  $R(r, m)$  and its covering radius, see [241], [242] and [223].

## 7.2 Covering Radius of BCH Codes

Consider the binary linear BCH code  $B(\tau, N, m)$  where  $\tau$  and  $N$  are natural numbers and  $N$  is a divisor of  $2^m - 1$ . This cyclic code is of length  $(2^m - 1)/N$  and its roots are the elements  $\alpha^N, \alpha^{3N}, \dots, \alpha^{(2\tau-1)N}$ , where  $\alpha \in GF(2^m)$  is a primitive element. Its generator polynomial is the least common multiple of

$$m_N(x), m_{3N}(x), \dots, m_{(2\tau-1)N}(x),$$

where  $m_i(x)$  stands for the minimum polynomial of  $\alpha^i$  over  $GF(2)$ . Denote its covering radius by  $\rho(\tau, N, m)$ . The best result in evaluating  $\rho$  was derived in [248]:

**Proposition 7.3** (a) *There exists a positive constant  $m_0$  dependent on  $\tau$  such that for  $m > m_0$*

$$\rho(\tau, 1, m) = 2\tau - 1;$$

(b) *For  $N \neq 1$  and  $m \geq (4\tau + 2)\log_2((2\tau - 1)N)$ ,  $\rho(\tau, N, m) = 2\tau$ .*

**Sketch of the proof of Proposition 7.3.** The lower bound in (a) is from the supercode lemma (see for instance [43, Prop. 1]) and the fact that  $B(\tau, 1, m) \subset B(\tau - 1, 1, m)$ . For the upper bound, we start with the following result of A. Tietäväinen [238], who refined an approach of [92].

**Proposition 7.4**  $\rho(\tau, N, m) \leq 2\tau$  if  $m \geq (4\tau + 2)\log_2((2\tau - 1)N)$ .

**Sketch of the proof of Proposition 7.4.** According to an equivalent definition, the covering radius is the least natural number  $t$  such that for any elements  $a_1, \dots, a_\tau \in GF(2^m)$ , the vector  $(a_1, \dots, a_\tau)^t$  is a linear combination with coefficients in  $GF(2)$  of at most  $t$  columns of the parity check matrix of the code  $B(\tau, N, m)$ . Since the parity check matrix has the form  $h_{ij} = \alpha^{j(2i-1)N}$ ,  $i = 1, \dots, \tau$ ;  $j = 1, \dots, (2^m - 1)/N$ ,  $\rho(\tau, N, m)$  does not exceed  $t$  if for any  $a_1, \dots, a_\tau \in GF(2^m)$ , the system

$$\sum_{j=1}^t x_j^{(2i-1)N} = a_i, \quad i = 1, \dots, \tau \tag{7.81}$$

has a solution in  $GF(2^m)$ . On the other hand, if (7.81) has no solution in  $GF(2^m)$  for some  $a_1, \dots, a_\tau$ , then  $\rho(\tau, N, m) > t$ .

Assume  $t = 2\tau$ . The main idea of [238] is to replace the system (7.81) of  $\tau$  non-homogeneous equations of  $2\tau$  variables by the system

$$\sum_{j=1}^{2\tau} x_j^{(2i-1)N} = a_i y^{(2i-1)N}, \quad y \in GF(2^m), y \neq 0, i = 1, \dots, \tau \quad (7.82)$$

of  $\tau$  homogeneous equations of  $2\tau + 1$  variables. Using the Carlitz-Uchiyama bound for exponential sums, Tietäväinen proved that (7.82) has a solution  $(x_1, \dots, x_{2\tau}, y)$ , and so (7.81) has the solution  $(y^{-1}x_1, \dots, y^{-1}x_{2\tau})$ , thus proving  $\rho(\tau, N, m) \leq 2\tau$  for  $m$  large enough.  $\square$

In [248], to prove (a), a deep result of Lang and Weil ([149]) was used instead of the Carlitz-Uchiyama bound for demonstrating the coincidence of the lower and upper bounds for sufficiently large  $m$  (unfortunately, estimating  $m_0$  in a reasonable way seems hardly possible now; see, however, the remark below). To prove (b), a vector  $(a_1, \dots, a_\tau)$ , such that (7.81) has no solution for  $N \neq 1$  and  $t \leq 2\tau - 1$ , was found. This gives, along with Proposition 7.4, the desired result.  $\square$

**Remark.** In [182] and [183], the elementary constructive approach of Stepanov and Schmidt was used to estimate  $m_0$  in Proposition 7.3(a) as

$$\log_2(10^4 \tau^3 d^5 P^3(\lfloor 4 \log_{10} d \rfloor)),$$

where  $d = (2\tau - 1)!!$ ;  $P(1) = 2, P(2) = 3, \dots$  is the sequence of primes.

Weaker restrictions on  $m$  for a weaker bound on  $\rho(\tau, 1, m)$  were derived in [57] by exploiting a relation between the covering radius and the dual distance of BCH codes (again the Carlitz-Uchiyama bound).

**Proposition 7.5** [57] *If  $m \geq (2\tau + 1)\log_2\left(\frac{(\tau-1)+2^{-m/2}}{1-2^{-m}}\right)$ , then  $\rho(\tau, 1, m) \leq 2\tau + 1$ .*  $\square$

We would also mention

**Proposition 7.6** [92] *If  $m \geq 7$ ,  $m$  odd, and  $\tau = 2^{m-3} - 1$ , then  $\rho(\tau, 1, m) \geq 2\tau + 1$ .*  $\square$

The following result was stated in [239] and proved in [240].

**Proposition 7.7** *If  $m \geq (4\tau - 2)\log_2(2\tau)$ , and  $\tau = 2^u + 1$ , then  $\rho(\tau, 1, m) = 2\tau - 1$ .*  $\square$

The following values are known for particular  $\tau$ :

$$\begin{array}{ll} \rho(1, 1, m) = 1 & \text{(Hamming code);} \\ \rho(2, 1, m) = 3 & [78]; \\ \rho(3, 1, m) = 5 & [118] \quad \text{for } m \equiv 0 \pmod{4}, \\ & [5] \quad \text{for } m \equiv 1, 3 \pmod{4}, \\ & [91] \quad \text{for } m \equiv 2 \pmod{4}. \end{array}$$

About BCH codes and normality, see Proposition 6.4.

### 7.3 Duals of BCH Codes

Duals of binary BCH codes have also received much attention (see [166]). Their minimum distance may be estimated using the Carlitz-Uchiyama bound [4].

Let  $C(\tau, m)$  be the dual of a binary primitive BCH code of length  $2^m - 1$  and designed distance  $2\tau + 1$ ,<sup>2</sup> and let  $\rho(\tau, m)$  be its covering radius.

**Proposition 7.8** [241], [242]

$$\rho(\tau, m) \leq 2^{m-1} - 1 - \left(\sqrt{\tau} - \sqrt[6]{\tau}\right) \sqrt{2^m - \tau - 2}.$$

□

The proof adapted Delsarte's methods [58] to show that  $\rho(\tau, m)$  was bounded above by the smallest zero of a Krawchouk polynomial. An improvement in the upper bound would yield improved lower bounds for character sums in fields of characteristic 2.

### 7.4 Covering Radius of Cyclic Codes

Consider a binary cyclic code of length  $(2^m - 1)/N$  with generator polynomial  $m_{i_1 N}(x)m_{i_2 N}(x) \dots m_{i_r N}(x)$  without multiple roots.

**Proposition 7.9** If  $m \geq (4\tau + 2)\log_2(N \max\{i_s; 1 \leq s \leq \tau\} - 1)$ , then the covering radius does not exceed  $2\tau$ . □

The proof (see [92], [238]) relies on A. Weil's bounds for exponential sums.

Finding the covering radius of a binary cyclic code with irreducible generator polynomial is equivalent to Waring's problem in  $GF(2^m)$  [92].

Some computer calculations were done to evaluate the covering radius of all cyclic codes of length up to 64 ([63], [64]). Many of these codes are optimal in the sense of having the smallest possible covering radius of any linear code of same length and dimension (i.e., they achieve  $t[n, k]$ ; see for instance in Table B the entries marked D).

For other bounds, see [246], [247].

### 7.5 Covering Radius of Binary Self-Dual Codes

The code  $C$  is called *self-dual* if  $C = C^\perp$ . If all weights in  $C$  are divisible by 4, then  $C$  is called *doubly even* and exists only when its length  $n$  is divisible by 8 [76]. *Extremal* doubly even codes have the weight distribution, given by the Gleason polynomials, of a self-dual code with the largest possible minimum weight. Their parameters are  $[8m, 4m, 4 \lfloor \frac{m}{3} \rfloor + 4]$ .

The covering radius of extremal doubly even self-dual codes was studied in [6]. Mainly by use of the Delsarte bound, the following bounds on covering radii were presented.

---

<sup>2</sup>The minimum distance of  $C(\tau, m)$  is at least  $2^{m-1} - (\tau - 1)2^{m/2}$  (see [166, Ch. 9, p. 281], and [158] for further improvements).

$n$	8	16	24	32	40	48	56	64
$t(C)$	2	2	4	6	6–8	8	8–10	8–12

**Proposition 7.10** [6]  $t(C) \leq 2m - 2 \left\lfloor \frac{m}{3} \right\rfloor$ .  $\square$

This is simply the Delsarte bound. The sphere-covering lower bound asymptotically yields

$$t(C) \gtrsim 8mH^{-1}(1/2) \approx 0.88m.$$

## 7.6 Covering Radius of Algebraic-Geometric Codes

We refer to [244] for definitions from algebraic geometry.

Let  $X$  be a smooth projective absolutely irreducible algebraic curve of genus  $g$  over  $GF(q)$ ,  $q = p^\ell$ , for the prime  $p$ . Let  $G$  be an effective divisor defined over  $GF(q)$  and  $L(G)$  be the space of rational functions defined over  $GF(q)$  whose divisor  $(f)$  is such that  $(f) + G$  is effective. Let  $\{P, Q_1, \dots, Q_n\}$  be the set of  $GF(q)$ -points of  $X$  outside the support of  $G$ , and let  $D = Q_1 + \dots + Q_n$ . Define  $\Gamma(D, G)$  to be the algebraic-geometric (AG) code over  $GF(q)$  of length  $n$  whose parity check matrix is  $h_{ij} = f_i(Q_j)$ , where the  $f_i$  form a basis of  $L(G)$ . The code  $\Gamma(D, G)$  has parameters  $[n, k = n - \deg(G) + g - 1, d \geq \deg(G) - 2g + 2]$ . Let  $G_1$  be the divisor of minimum degree such that  $0 < G_1 \leq G$ . Then, from the supercode lemma,  $t(\Gamma(D, G)) \geq d(\Gamma(D, G - G_1))$ , and the following result holds.

**Proposition 7.11** [130]  $t(\Gamma(D, G)) \geq \deg(G) - \deg(G_1) - 2g + 2$ .  $\square$

In [130], [131] upper bounds for covering radius were used for demonstrating optimality of several subclasses of AG codes. Weierstrass gaps of points were used in [131] to improve the lower bounds on  $t(\Gamma(D, G))$ .

Consider now the covering radius of subfield subcodes of AG codes. This includes the cases of BCH codes and Goppa codes. We will follow the paper of Skorobogatov [219].

Define  $\Gamma(D, G - P)$  analogously to  $\Gamma(D, G)$ . Note that  $\Gamma(D, G)$  is the subcode of  $\Gamma(D, G - P)$  consisting of vectors with sum of coordinates equal zero. Let  $S(D, G - P)$  and  $S(D, G)$  be the subfield subcodes over  $GF(p)$  of  $\Gamma(D, G - P)$  and  $\Gamma(D, G)$ , respectively. The code  $S(D, G - P)$  coincides with a primitive narrow-sense BCH code when  $X = \mathbb{P}^1$ ,  $P = \{0\}$ , if  $G$  is a multiple of the infinite point  $\{\infty\}$ , and with a classical Goppa code when  $X = \mathbb{P}^1$ ,  $P = \{\infty\}$ , if  $G$  is an arbitrary effective divisor with support disjoint from  $P$ .

For the following proposition, define  $G_2$  to be the divisor of maximum degree such that  $0 \leq pG_2 \leq G$ . Denote by  $s$  the number of points in  $\text{supp}(G)$ , defined over the algebraic closure of  $GF(q)$ , and  $r := \dim L(G - P) - \dim L(G_2 - P)$ ; in particular,  $r = \deg(G) - \deg(G_2)$  if  $\deg(G_2 - P) > 2g - 2$  (from the Riemann-Roch theorem).

**Proposition 7.12** [180], [181] for  $p = 2$ , [219]. Assume that one of the following two conditions holds:

1.  $n > ((2g - 2 + s + \deg(G))p^{\ell/2} + s + 1)p^{\ell r/(2r+1)}$ ;

$$2. \ell > (4r + 2)\log_p(2g + s + 1 + \deg(G)),$$

then  $t(S(D, G - P)) \leq 2r + 1$ ,

$$t(S(D, G)) \leq 2r + 1, \text{ for } p \neq 2,$$

$$t(S(D, G)) \leq 2r + 2, \text{ for } p = 2.$$

□

## 8 Covering Radius and Dual Distance

The covering radius of a code depends heavily on its dual distance. This fact was mentioned long ago [93], but there has been a recent revival of interest in the problem of finding upper bounds on the covering radius as a function of its dual spectrum. For earlier results on the problem, such as “Norse bounds,” etc., see Section III.D of the previous survey [43]. The Norse bounds were generalized in [223],[225], where the closeness of the weight distribution of the cosets of a code to the binomial distribution was exploited. Actually, these distributions have identical first  $(d' - 1)$  moments, where  $d'$  is the dual distance of the code. It allows estimating from above the weight of the first nonzero element of the weight spectrum of the cosets, which is evidently equal to the covering radius of the code.

A. Tietäväinen proved in [241],[242] the following bound on  $\rho := t(C)/n$  as a function of  $\delta' := d'/n$ :

$$\rho \leq 1/2 - 1/2\sqrt{\delta'(2 - \delta')}. \quad (8.83)$$

On the other hand, since almost all codes satisfy asymptotically the Gilbert-Varshamov bound, there exists a sequence of codes such that

$$\rho \geq H^{-1}(1 - H(\delta')). \quad (8.84)$$

In [57],[226], improvements on (8.83) were obtained for a particular range of  $\delta'$  close to  $1/2$  under different additional assumptions, such as linearity, bounded dual-distance width, etc.

Finally, it was shown in [159] that the Tietäväinen and Solé-Stokes [226] bounds could be derived as the result of a uniform approach. We state the main result of [159] in the next proposition.

Let  $P_i(x)$  be the  $i$ -th Krawchouk polynomial,  $A(n, d)$  be the maximal size of a code of length  $n$  and minimum distance  $d$ ,  $A^*(n, d)$  be the upper linear programming bound for the maximal size of a code of length  $n$  and minimum distance  $d$ ,  $A(n, d, w)$  be the maximal size of a constant weight  $w$  code of length  $n$  and minimum distance  $d$ , and  $R(n, d')$  be the maximal covering radius of a code of length  $n$  and dual distance  $d'$ .

**Proposition 8.1** [159] (a) *Let  $r$  be an integer and suppose the polynomial*

$$\alpha(x) = \sum_{i=0}^n \alpha_i P_i(x)$$

*satisfies*

- $\alpha(0) > n \cdot \max \{ |\alpha(w)| \cdot A(n, d', w) \}$  *for linear codes ;*

- $\alpha(0) > n\sqrt{A^*(n, d')} \cdot \max \left\{ |\alpha(w)| \cdot \sqrt{\binom{n}{w}} \right\}$  for unrestricted nonlinear codes ;
- $\alpha_i \leq 0$  for  $i = r + 1, \dots, n$ .

Then  $R(n, d') \leq r$ .

(b) (Dual statement)

Let  $r$  be an integer and suppose the polynomial

$$\beta(x) = \sum_{i=0}^n \beta_i P_i(x)$$

satisfies

- $\beta_0 > n \cdot \max \{ |\beta_w| \cdot A(n, d', w) \}$  for linear codes ;
- $\beta_0 > n\sqrt{A^*(n, d')} \cdot \max \left\{ |\beta_w| \cdot \sqrt{\binom{n}{w}} \right\}$  for unrestricted nonlinear codes ;
- $\beta(i) \leq 0$  for  $i = r + 1, \dots, n$ .

Then  $R(n, d') \leq r$ . □

Particular choices of polynomials in Proposition 8.1 lead to different bounds. If one chooses  $\beta_i = 0$  for  $i \geq d'$ , then a polynomial proposed in [148] leads to (8.83). For the choice  $\alpha(x) = (P_a(x))^b$  for some integers  $a$  and  $b$  we get the Delorme-Solé-Stokes bounds. Note that in Proposition 8.1, for

$$\max \{ |\alpha(w)| \cdot A(n, d', w) \}$$

we may substitute

$$A(n, d') \cdot \max \{ |\alpha(w)| \}.$$

Hence using appropriate Tchebysheff polynomials (see [159]) gives the following bound for linear codes:

$$\rho \leq \frac{H\left(\frac{1}{2} - \sqrt{\delta'(1 - \delta')}\right)}{\log_2(e) \cosh^{-1}\left(\frac{1+\delta'}{1-\delta'}\right)}. \quad (8.85)$$

Let us mention that the Delsarte bound [58] (the covering radius is at most the number of non-zero elements in the dual spectrum) may be derived from the above proposition for a particular choice of the polynomial. Thus, it always gives a result at least as good as that of Delsarte's theorem.

In [70] the results of Tietäväinen were generalized to other metric spaces.

## 9 Generalizations of Coverings

The notion of covering has been generalized in several ways. The main source for these generalizations was the so-called *football pool problem* (cf. Section 2.7). Its goal is to find a way of forecasting the outcome of  $n$  football matches with a fixed maximal number,  $t$ , of wrong outcomes in at least one guess, using a minimal number of guesses; thus you are sure to win at least the  $(t + 1)$ -st prize, no matter what the actual outcomes are. When ties are possible, this problem coincides with the problem of constructing minimal  $t$ -coverings in a ternary Hamming space of length  $n$ . However, some initial knowledge about possibilities of outcomes can reduce this problem to that of covering some subset of the ternary Hamming space, namely a mixed binary-ternary space.

We now give a survey of some problems related to football pool problems.

### 9.1 Mixed Coverings

Mixed coverings were introduced in Section 2.7.2. Some lower bounds were given in Section 2.7.2, and upper bounds in Section 5.7.2.

We recall the notation. For  $i = 1, 2, \dots, n$ , let  $Q_i$  be an alphabet consisting of  $q_i \geq 2$  symbols, and let  $V$  be the Cartesian product  $V := Q_1 \times Q_2 \times \dots \times Q_n$ . If  $e$  is a nonnegative integer,  $B_e(x)$  denotes the sphere with radius  $e$  and center  $x$ :  $B_e(x) = \{y \in V, d(x, y) \leq e\}$ . A code  $C \subset V$  is a *perfect mixed  $e$ -code* if the spheres  $B_e(c)$ ,  $c \in C$ , form a partition of  $V$ .

The earliest publication on perfect mixed codes seems to be the conference paper by Schönheim [215]. Later on, perfect  $e$ -codes were studied by Herzog and Schönheim [95],[96], Lenstra [151], Heden [89],[90], Lindström [153] and Reuvers [208]. Except for [89] and [208], those cited deal mostly with the case that the  $q_i$  are all powers of the same prime and  $e = 1$ . By [95, Th. 1], a 1-code can be constructed from an abelian group that has a certain partitioning property. As a consequence of [95, Th. 2], which gives sufficient conditions for a class of abelian groups to have that partitioning property, one can easily find many perfect 1-codes.

**Example 9.1** Let  $q$  be a prime power and let  $\alpha$  and  $m$  be integers with  $m > \alpha \geq 2$ , and put  $n = 1 + (q^m - q^\alpha)/(q - 1)$ . Then there exists a 1-code in  $\mathbf{F}_{q^\alpha} \times \mathbf{F}_q^{n-1}$ , which moreover is a subgroup of  $\mathbf{F}_{q^\alpha} \times \mathbf{F}_q^{n-1}$  (viewed as an additive group).

In [89] and [208, Ch. 6], perfect mixed  $e$ -codes are treated with  $e$  and the  $q_i$  arbitrary. Reuvers [208] proved the nonexistence of certain perfect mixed 2- and 3-codes. It was not known if there were any perfect mixed  $e$ -codes with  $e > 1$ . But for  $e = 2$  [67] such a family of codes was constructed by Etzion and Greenberg. These codes have length  $2^{2m} + 1$ , size  $2^{2^{2m} - 2m - 1}$  and are constructed over alphabets  $Q_1 = Q_2 = \dots = Q_{2^{2m}} = \mathbf{F}_2$ ,  $Q_{2^{2m}+1} = \mathbf{F}_{2^{2m-1}}$ . They consist of words  $c = (x|i)$ , where  $x$  is a word of the extended Hamming code of length  $2^{2m}$ , and  $i$  is the number of the coset of the Preparata code of the corresponding length in the Hamming code.

Non-existence theorems for perfect mixed codes are derived in [252],[67].



Constructions of mixed codes were studied mostly for the binary/ternary case (see [252], [157], [190], [85], [192], [194]). Lower bounds improving on the sphere-covering bound were derived in [252]. Actually, as was mentioned in [190], we can construct good binary coverings from mixed coverings. This construction was further generalized in [67], [42]. We quote [67]:

A *covering by coverings* (CBC) of  $\mathbf{F}^n$  is a set of  $(n, t)_1$  codes for which the union is equal to  $\mathbf{F}^n$ .

*Construction:* Let  $C$  be a code over  $V = \mathbf{F}_{k_1}^{n_1} \times \mathbf{F}_{k_2}^{n_2} \times \cdots \times \mathbf{F}_{k_r}^{n_r}$  with radius  $t$ . Let  $C_0^i, C_1^i, \dots, C_{k_i-1}^i, 1 \leq i \leq r$ , be  $r$  CBC's. Then construct a new code by encoding  $C$  using the sets of rules  $j \rightarrow C_j^i$  for  $1 \leq i \leq r, j \in \mathbf{F}_{k_i}$ , in each coordinate in all possible ways.

The code obtained has covering radius  $t$ .

In particular, application of this construction to perfect mixed codes leads to some new records (see [67]). Östergård [190] constructed a mixed code over  $\mathbf{F}_4 \times \mathbf{F}_2^7$  of covering radius 1 with 60 words. This code corresponds to a binary  $(10, 120)_1$  covering—a record.

## 9.2 Weighted Coverings

The notion of weighted coverings proved to be very fruitful. Many perfect configurations such as classical perfect codes, uniformly packed codes,  $L$ -codes, etc., are particular cases of weighted coverings. (For details and applications, see [42]).

Let us introduce the weighted covering problem rigorously. For  $x \in \mathbf{F}^n$ ,  $A_C(x) = (A_0(x), A_1(x), \dots, A_n(x))$  will stand for the distance distribution of  $C$  with respect to  $x$ ; thus

$$A_i(x) := |\{c \in C; d(c, x) = i\}|.$$

For any  $(n+1)$ -tuple  $M = (m_0, m_1, \dots, m_n)$  of rational numbers—the  $m_i$  are the weights—we define the  $M$ -density of  $C$  at  $x$  as

$$\langle M, A_C(x) \rangle := \sum_{i=0}^n m_i A_i(x).$$

We consider  $M$ -coverings, i.e., codes  $C$  such that  $\langle M, A_C(x) \rangle \geq 1$  for all  $x$ .

$C$  is a *perfect  $M$ -covering* if  $\langle M, A_C(x) \rangle = 1$  for all  $x$ .

We define the *diameter* of an  $M$ -covering as

$$\delta := \max\{i; m_i \neq 0\}.$$

One way of seeing a weighted covering is as a union of weighted spheres (i.e., spheres with different weights attached to their layers) around the codewords such that the accumulated density in every point of the space is at least 1. The case  $m_0 = \cdots = m_\delta = 1$  corresponds to the classical case.

Classification of perfect weighted coverings of small diameter was made in [45], [46], [41], [42]. In these papers some general methods for constructing such  $M$ -coverings were proposed. Some particular cases were studied in more detail.

### 9.2.1 Multiple Coverings

This is the case when  $m_0 = \dots = m_\delta = 1/\mu$ . It means that every point of the space is covered by at least  $\mu$  spheres (in terms of football pools, you are sure to win  $\mu$  prizes, each of which is at least the  $(t(C) + 1)$ -st prize). Perfect multiple coverings were studied in [34],[255] in the binary and non-binary cases. It was shown that there exist perfect multiple coverings which are not a union of cosets of a conventional perfect covering. Complete classification of such perfect coverings is still an open problem. Honkala [108] generalized the notion of normality to multiple coverings. Upper and lower bounds were extensively studied in [82], with a table of bounds for  $n \leq 16, t \leq 4$ , and  $\mu \leq 4$ .

Results on generalizations to schemes other than Hamming association schemes may be found in [34].

### 9.2.2 Multiple Coverings of the Farthest-Off Points

This topic corresponds to weighted coverings with  $m_0 = \dots = m_{\delta-1} = 1, m_\delta = 1/\mu$ : every vector  $z \in \mathbb{F}^n$  satisfies  $d(z, C) \leq \delta$  (so  $t(C) \leq \delta$ ), and if  $d(z, C) = \delta$  (the set of such points may be empty), then  $z$  is covered by at least  $\mu$  codewords (in terms of football pools, you are sure to win at least the  $t(C)$ -th prize or at least  $\mu$  times the  $(t(C) + 1)$ -st prize). Constructions of such codes and tables for  $n \leq 16, t \leq 4, \mu \leq 4$  may be found in [83].

## 10 Open Problems

Let us first review the status of some of the 15 problems listed in [43] and then add two conjectures that have since appeared in the literature (see Problems 16 and 17). We also add a new problem, 18. The numbering follows [43]. We omit most of those problems on which there has been little or no progress.

3. We quote from [43]: “It would be interesting to find more values of  $K(n, \rho)$ ”.

See Table A for exact values and bounds on  $K(n, \rho)$  for  $1 \leq n \leq 33, 1 \leq \rho \leq 10$ .

5. Is it true that  $t[n + 2, k] \leq t[n, k] + 1$  for all  $n, k$ ?

This is still open. It has been proved for  $n - k = o(n)$ , or  $k = o(n)$  [139, I], or whenever  $t[n, k]$  is realized by a subnormal code [102] (cf. Section 6.4).

7. For  $K = 2^k$ , is  $t(n, K)$  always attained by a linear code?

The answer is “No” [67]. One combines  $K(23, 2) \leq 2^{15}$  ([67]; cf. Table A), which gives  $t(23, 2^{15}) = 2$ , and  $t[23, 15] = 3$  ([29]; cf. Table B).

8. For all  $n, k$ , is there a code  $C$  realizing  $t[n, k]$  with  $1^n \in C$ ?

The answer is “No” [61], because  $t[14, 6] = 3$ , but any  $[14, 6]$  code containing  $1^{14}$  has covering radius at least 4.

9. For fixed  $k$  is it true that  $(n/2 - t[n, k])2^{-k/2} = \Theta(1)$ ?

This is proved in [79].

12. It was conjectured that for  $m > m_0(e)$ ,  $t(\text{BCH}_e) = 2e - 1$ .

This was proved in [218] (cf. Section 7.2, Proposition 7.3(a)).

13. Is  $t[2s + 1, 4] = s - 2$  for  $s \geq 3$ ?

This was proved in [79], where  $t[n, 5] = \lfloor (n - 5)/2 \rfloor$  for  $n \geq 5, n \neq 6$ , was also established (see Section 2.6.2). Furthermore, Graham and Sloane conjectured [79] that :

For all  $m$ , and for  $n$  large enough,

$$\begin{aligned} t[n, 2m] &= \lfloor (n - 2^m)/2 \rfloor \\ t[n, 2m + 1] &= \lfloor (n - 2^m - 1)/2 \rfloor. \end{aligned}$$

(Presumably they meant to say “for all  $m \geq 2$ ,” since the known values of  $t[n, k]$  for  $k \leq 3$  disagree with the conjectured values.) They proved the conjectured values are upper bounds for  $m = 3$  (i.e.,  $k = 6$  and  $k = 7$ ) and  $n \geq 19$ , and recently Hou did the same for  $k = 8$  [127]. If true, their conjecture would imply

$$t[n + 1, 2m + 1] = t[n, 2m] = \left\lfloor \frac{n}{2} \right\rfloor - 2^{m-1},$$

$$t[n + 1, 2m + 2] = \left\lfloor \frac{n + 1}{2} \right\rfloor - 2^m,$$

and finally

$$t[n, 2m + 1] = t[n + 1, 2m + 2] + 2^{m-1} - 1$$

(compare with inequality (10.87) below).

We now mention two more conjectures; we disprove the first one (Problem 16), the second one is still open (Problem 17).

#### 16. Disproof of a conjecture.

For fixed redundancy  $m := n - k$ , the entries in a table of  $t[n, k]$  are on a diagonal parallel to the main diagonal. As  $n$  increases we move down the diagonal, and  $t[n, n - m]$  is nonincreasing. Typically  $t[n, n - m]$  remains constant for several consecutive values of  $n$  and then drops (it drops by 1 in every case in which both exact values are known in Table B). These points of change signal a value of the *length function*,  $\ell$ , introduced in [24]: if  $t[n - 1, n - 1 - m] > t[n, n - m] =: t_0$ , then  $\ell(m, t_0) = n$ . In other words,  $\ell(m, t)$  is defined as the smallest value of  $n$  for which there is a binary linear  $[n, n - m]$  code with covering radius  $t$  (see [162] for a short survey and a table for the length function).

It was conjectured in [24, p. 108] that

$$\text{for all } m \text{ and } t \text{ such that } 1 \leq t \leq \lceil m/2 \rceil - 1, \ell(m, t) > \ell(m, t + 1). \quad (10.86)$$

We can see immediately that this conjecture is equivalent to saying that the drop in  $t[n, n - m]$ , for constant  $m$ , is at most 1 (when  $n$  increases by 1) as long as  $1 \leq t[n, n - m] \leq \lceil m/2 \rceil - 1$ , or, equivalently,

$$t[n, k] \leq t[n + 1, k + 1] + 1, \text{ for } n \geq k \geq 1. \quad (10.87)$$

We now disprove this conjecture, by proving:

**Theorem 10.1** *For all  $k \geq 14$  and all  $n \geq 2^{k-2}$ , there is at least one value  $t[n, j]$ , with  $2 \leq j \leq k$ , such that  $t[n - 1, j - 1] \geq 2 + t[n, j]$ .*

**Proof.** Using the bound on  $t[n, k]$  established in [43, (31)], we have, for all  $k \geq 3$  and for  $n \geq 2^{k-2}$ ,

$$t[n, 1] - t[n, k] \geq \lceil 2^{(k-4)/2} \rceil. \quad (10.88)$$

It follows from Proposition 5.1 that for all  $n$  and  $j$  ( $n \geq 2$ ,  $j \geq 1$ ,  $n \geq j$ ),

$$t[n-1, j-1] + 1 \geq t[n, j-1]. \quad (10.89)$$

Now choose  $n$  and  $k$  satisfying the hypotheses of the theorem and assume the contrary of our desired conclusion, that for all  $j$  with  $2 \leq j \leq k$ ,

$$t[n, j] + 1 \geq t[n-1, j-1]. \quad (10.90)$$

Adding (10.89) and (10.90), we see that for all  $j$  with  $2 \leq j \leq k$ ,

$$t[n, j-1] - t[n, j] \leq 2. \quad (10.91)$$

We estimate the left-hand side of (10.88) using (10.91):

$$t[n, 1] - t[n, k] = \sum_{1 \leq i < k} (t[n, i] - t[n, i+1]) \leq 2(k-1). \quad (10.92)$$

Inequalities (10.88) and (10.92) imply

$$\lceil 2^{(k-4)/2} \rceil \leq t[n, 1] - t[n, k] \leq 2(k-1). \quad (10.93)$$

Inequality (10.93) fails if  $k \geq 14$ . Therefore the conjecture fails.  $\square$

In fact, we proved there are infinitely many arbitrarily long strings

$$\ell(m, t) = \ell(m, t+1) = \dots = \ell(m, t+b) :$$

**Corollary 10.1** *For each integer  $b \geq 1$ , for all  $k$  such that  $\lceil 2^{(k-4)/2} \rceil / (k-1) > b+1$  and for all  $n \geq 2^{k-2}$ , there is at least one value  $t[n, j]$  with  $2 \leq j \leq k$  such that*

$$t[n-1, j-1] \geq b+1 + t[n, j].$$

*For such  $j$ , with  $t_0 := t[n, j]$ ,  $\ell(n-j, t_0) = \ell(n-j, t_0+1) = \dots = \ell(n-j, t_0+b)$ .*  $\square$

17. The following conjecture was stated in [47]:

**Conjecture 10.1** Among optimal covering codes (i.e.,  $(n, K(n, t))t$  codes), there is at least one that is balanced (see Section 2.3).

18. Prove or disprove that every binary linear code is normal. See Section 6.1 for discussion.

**Table A.** Table of lower and upper bounds for  $K(n, t)$ ,  $1 \leq n \leq 33, 1 \leq t \leq 10$ .

As often as possible, we mention the *earliest* reference. All upper bounds can be obtained by a normal code (except maybe  $K(21, 2)$  and  $K(22, 2)$ ). All DS and possible ADS have been computed. Let us remark that there are normal codes whose acceptable coordinates have unbalanced columns (cf. Section 2.3). Examples are the  $(11, 44)2, (9, 62)1, (10, 120)1$  codes. The ADS of such a code with a code of odd cardinality, or with another such code, leads to a smaller cardinality for the resulting code; however, we didn't find any case where this leads to further improvements on upper bounds for  $K(n, t)$ .

**Key to Table A:**

p = perfect codes.

q = [230], [231].

r = [47].

t = [102].

**lower bounds:**

unmarked = trivial.

s = sphere-covering bound.

b = [250].

c = [156].

d = [119].

e = [265], [266].

f = [152].

g = [254].

h = [107].

i = [80].

j = [110].

**upper bounds:**

unmarked = trivial, from the direct sum of two codes, from Corollary 5.1, from the amalgamated direct sum of a (sub)normal code and a repetition code of odd length (cf. Section 5.3, Example 5.2), or from a linear code (cf. Table B).

A = amalgamated direct sum with two of the following codes:  $(5, 7)1, (6, 12)1, (7, 16)1, (9, 62)1, (10, 120)1, (11, 192)1, (12, 380)1, (15, 2048)1, (19, 31744)1, (10, 30)2, (11, 44)2, (13, 128)2, (15, 480)2, (12, 28)3, (13, 42)3, (14, 64)3, (15, 112)3, (16, 192)3, (23, 4096)3, (15, 40)4, (19, 64)5$ .

B = [257], [258].

C = [112].

D = Section 5.4.

E = [82].

F = [85] (includes results previously published in football pool magazines).

G = [192].

H = [67].

J = [199].

K = [83].

L = [197].

M = [200].

$n$	$t = 1$	$t = 2$	$t = 3$	$t = 4$
1	1			
2	2	1		
3	2	2	1	
4	s 4	2	2	1
5	q 7 q	2	2	2
6	q 12 q	r 4	2	2
7	p 16 p	r 7	2	2
8	q 32	e 11–12	r 4	2
9	i 55–62 B	f 15–16	r 7	2
10	e 105–120 B	c 23–30 F	e 9–12	r 4
11	g 177–192 F	e 36–44 F	d 12–16	r 7
12	b 342–380 J	b 61–78 G	e 18–28 E	t 8–12
13	r 598–736 M	t 97–128	f 28–42 E	e 11–16
14	b 1171–1408 L	r 157–256	f 44–64	t 15–28
15	p $2^{11}$ p	f 309–480 E	f 70–112 C	e 22–40 E
16	b $2^{12}$	e 512–896 E	e 114–192 K	e 33–64
17	h $7399 \cdot 2^{13}$	r 859–1536 A	e 186–352 A	f 52–112
18	b $14564 \cdot 2^{14}$	e 1702–3040 A	e 316–512	e 83–192
19	j $26236 \cdot 31 \cdot 2^{10}$ D	t $2897 \cdot 2^{12}$	e $511 \cdot 2^{10}$	f 128–332 C
20	b $52429 \cdot 31 \cdot 2^{11}$	e $5328 \cdot 2^{13}$	b $889 \cdot 2^{11}$	f 208–512
21	i $95330 \cdot 15 \cdot 2^{13}$ t	b $9893 \cdot 7 \cdot 2^{11}$ H	t $1475 \cdot 3840$ A	f 336–896 A
22	b $190651 \cdot 15 \cdot 2^{14}$	e $17316 \cdot 3 \cdot 2^{13}$ H	f $2539 \cdot 2^{12}$	f 553–1536 A
23	e $352063 \cdot 3 \cdot 2^{17}$ r	f $30677 \cdot 2^{15}$ H	p $2^{12}$ p	f 902–2816 A
24	b $699051 \cdot 3 \cdot 2^{18}$	b $60350 \cdot 2^{16}$	e $8123 \cdot 2^{13}$	f $1505 \cdot 2^{12}$
25	i $1290562 \cdot 95 \cdot 2^{14}$	t $107203 \cdot 2^{17}$	e $13896 \cdot 2^{14}$	e $2554 \cdot 2^{12}$
26	b $2581111 \cdot 95 \cdot 2^{15}$	f $190775 \cdot 2^{18}$	e $23718 \cdot 2^{15}$	f $4263 \cdot 2^{13}$
27	j $4793563 \cdot 23 \cdot 2^{18}$	f $380328 \cdot 2^{19}$	e $40675 \cdot 2^{16}$	f $7176 \cdot 7 \cdot 2^{11}$ A
28	b $9586981 \cdot 23 \cdot 2^{19}$	t $683910 \cdot 2^{20}$	e $80720 \cdot 2^{17}$	f $12267 \cdot 3 \cdot 2^{13}$ A
29	b $17977788 \cdot 11 \cdot 2^{21}$	s $1231356 \cdot 2^{21}$	t $140567 \cdot 2^{18}$	f $21098 \cdot 2^{15}$
30	b $35791395 \cdot 11 \cdot 2^{22}$	f $2461754 \cdot 2^{22}$	t $248218 \cdot 2^{19}$	b $37973 \cdot 2^{16}$
31	p $2^{26}$ p	t $4464613 \cdot 2^{23}$	f $443248 \cdot 2^{19}$ H	t $64680 \cdot 31 \cdot 2^{12}$ A
32	b $2^{27}$	f $8168458 \cdot 2^{24}$	b $854890 \cdot 2^{20}$	t $110215 \cdot 15 \cdot 2^{14}$ A
33	i $252645140 \cdot 2^{28}$	b $16207424 \cdot 31 \cdot 2^{20}$ A	t $1516050 \cdot 2^{21}$	t $188678 \cdot 3 \cdot 2^{17}$ A

$n$	$t = 5$	$t = 6$	$t = 7$	$t = 8$	$t = 9$	$t = 10$
5	1					
6	2	1				
7	2	2	1			
8	2	2	2	1		
9	2	2	2	2	1	
10	2	2	2	2	2	1
11	2	2	2	2	2	2
12	r 4	2	2	2	2	2
13	r 7	2	2	2	2	2
14	t 8-12	r 4	2	2	2	2
15	t 9-16	r 7	2	2	2	2
16	t 13-28	t 8-12	r 4	2	2	2
17	e 19-40	c 8-16	r 7	2	2	2
18	e 27-64	t 11-28	t 8-12	r 4	2	2
19	e 40-64	e 16-40	c 8-16	r 7	2	2
20	f 62-128	e 23-64	t 10-28	t 8-12	r 4	2
21	f 95-256	f 33-64	e 14-40	c 8-16	r 7	2
22	f 150-512	f 49-128	f 20-64	t 9-28	t 8-12	r 4
23	f 235-880 C	f 73-224 A	f 29-64	e 13-40	c 8-16	r 7
24	f 376-1408 A	f 113-384 A	f 41-128	e 18-64	e 9-28	t 8-12
25	f 608-2464 A	f 172-512	f 60-224	f 25-64	e 12-40	c 8-16
26	f 981-2 <sup>12</sup>	e 272-2 <sup>10</sup>	f 88-384	f 35-128	e 16-64	b 8-28
27	f 1601-2 <sup>12</sup>	f 419-1984 A	f 132-512	f 50-224	f 22-64	e 11-40
28	f 2629-2 <sup>13</sup>	f 663-3584 A	f 202-960 A	f 73-384	t 30-128	t 14-64
29	f 4354-7 · 2 <sup>11</sup>	f 1068-2 <sup>12</sup>	f 311-1408 A	f 106-512	e 42-224	e 19-64
30	f 7307-3 · 2 <sup>13</sup>	f 1727-2 <sup>13</sup>	f 483-2 <sup>11</sup>	f 158-896 A	f 61-384	f 27-128
31	f 12220-2 <sup>15</sup>	f 2808-7 · 2 <sup>11</sup>	f 743-2 <sup>11</sup>	f 238-1344 A	f 88-512	t 37-224
32	f 20556-15 · 2 <sup>12</sup> A	f 4597-3 · 2 <sup>13</sup>	f 1179-2 <sup>12</sup>	f 366-2 <sup>11</sup>	f 127-896	e 51-384
33	f 34731-11 · 2 <sup>13</sup> A	f 7476-2 <sup>15</sup>	f 1878-2 <sup>13</sup>	f 557-2 <sup>11</sup>	f 188-1280 A	f 74-512

**Table B.** Table of lower and upper bounds for  $t[n, k]$ ,  $1 \leq n \leq 64$ ,  $1 \leq k \leq n$ .

As often as possible, we mention the *earliest* reference. All upper bounds can be obtained by a normal code. All DS and ADS have been computed.

**Key to Table B:**

q = [24]. r = [22].

**lower bounds:**

unmarked = sphere-covering bound.

n = from the nonlinear case (cf. Table A for  $n \leq 33$  and [266], [267] for  $34 \leq n \leq 64$ ).

b = [29]. c = [216].

d = [119], [121], [122]. e = [259].

f = [267]. g = [232], [233], [235], [234].

**upper bounds:**

unmarked = trivial or from the direct sum of two codes or [43] for  $n \leq 32$  or [79] for  $33 \leq n \leq 64$ .

A = amalgamated direct sum with two of the following codes: [15, 11]1, [26, 18]2, [39, 30]2, [18, 9]3, [23, 12]3, [38, 26]3, [45, 23]6, [31, 11]7.

B = [79]. C = [50], [52], [53], [54], [55], [75].

D = [63].

For small  $k$ , we remind the reader that we have (see Section 2.6.2):

$t[n, 1] = \lfloor n/2 \rfloor$  for  $n \geq 1$ ;  $t[n, 2] = \lfloor (n-1)/2 \rfloor$  for  $n \geq 2$ ;  $t[n, 3] = \lfloor (n-2)/2 \rfloor$  for  $n \geq 3$ ;  
 $t[n, 4] = \lfloor (n-4)/2 \rfloor$  for  $n \geq 4$ ,  $n \neq 5$ , and  $t[5, 4] = 1$ ;  $t[n, 5] = \lfloor (n-5)/2 \rfloor$  for  $n \geq 5$ ,  $n \neq 6$ ,  
and  $t[6, 5] = 1$ .

To save space, we give here some results for small codimension  $n - k$ :

$t[n, n] = 0$ , for  $n \geq 1$ ;  $t[n, n-1] = 1$ , for  $n \geq 2$ ;  $t[n, n-2] = 1$ , for  $n \geq 3$ ;  $t[n, n-3] = 1$ ,  
for  $n \geq 7$ ;  $t[n, n-4] = 2$ , for  $14 \geq n \geq 5$ , and  $t[n, n-4] = 1$ , for  $n \geq 15$ ;  $t[n, n-5] = 2$ , for  
 $30 \geq n \geq 9$ , and  $t[n, n-5] = 1$ , for  $n \geq 31$ ;  $t[12, 6] = 3$ ,  $t[n, n-6] = 2$ , for  $62 \geq n \geq 14$ , and  
 $t[n, n-6] = 1$ , for  $n \geq 63$ ;  $t[n, n-7] = 2$ , for  $64 \geq n \geq 21$ ;  $t[n, n-8] = 2$ , for  $64 \geq n \geq 30$ ;  
 $t[n, n-9] = 2$ , for  $64 \geq n \geq 44$ .



$k \setminus n$	13	14	15	16	17	18	19	20	21	22
6	3	3	c4	4B	4-5	5	5B	d6	6	6-7
7	2B	3	3	g4	4	4-5	4-5	5	5-6	n6
8			3	3	3-4	4	4-5	4-5	5	5-6
9				b3	3	3r	d4	4B	4-5	n5
10					b3	3	3	g4	4	4-5
11						e3	3	3	3-4	4
12							2B	3	3	3
13								2B	3	3
14										3

$k \setminus n$	23	24	25	26	27	28	29	30	31	32
6	n7	7-8	7-8	8-9	8-9B	n9-10	9-10	9-11	10-11	10-12
7	6-7	6-7	7-8	7-8	n8-9	8-9	8-10	n9-10	9-11	9-11
8	5-6	6-7	6-7	n7-8	7-8	7-9	n8-9	8-10	8-10	9-11
9	5-6	5-6	n6B	6-7	6-7B	7-8	7-8B	7-9	8-9B	8-10
10	4-5	5-6	5-6	g6B	6-7	6-7B	n7-8	7-8B	7-9	n8-9
11	4-5	4-5	5-6	5-6	5-6B	6-7	6-7B	6-7B	7B	7-8B
12	3	4	4	n5	5B	5-6	n6B	6-7	6-7B	n7B
13	3	3	4	4	4-5	5	5-6	5-6	6-7	6-7
14	3	3	3	4	4	4-5	5	5-6	5-6	6-7
15	b3	3	3	3	4	4	4B	5	5	5-6
16		g3	3	3	3	4	4	4	g5	5
17			2-3	3	3	3	4	4	4	4-5
18				2r	3	3	3	d4	4	4
19					2q	3	3	3	3-4	4
20						2B	3	3	3	3-4
21							2B	3	3	3
22									3	3
23										q3

$k \setminus n$	33	34	35	36	37	38	39	40	41	42
6	n11-12	11-13	11-13	12-14	12-14	d13-15	13-15	d14-16	14-16	14-17
7	10-12	10-12	n11-13	11-13	11-14	12-14	12-15	n13-15	13-16	n14-16
8	9-11	n10-12	10-12	10-13	11-13	11-14	n12-14	12-15	12-15	n13-16
9	n9-10	9-11	9-11	d10-12	10-12	10-13	11-13	11-14	n12-14	12-15
10	8-10	8-10	9-11	9-11	9-12	10-12	10-13	d11-13	11-14	11-14
11	7-8	8-9	8-9	n9-10	9-10	9-11	n10-11	10-12	10-12	11-13
12	7-8	7-8	n8-9	8-9	8-10	9-10	9-11	9-11	10-12	10-12
13	6-7	7-8	7-8	g8-9	8-9	8-10	n9-10	9-11	9-11	n10-12
14	6-7	6-7	7-8	7-8	7-8	8-9	8-9	8-10	9-10	9-11
15	n6	6-7	6-7	f7-8	7-8	7-8	d8-9	8-9	8-10	d9-10
16	5-6	5-6	6-7	6-7	6-8	7-8	7-8	7-9	8-9	8-10
17	5	5-6	5-6	6	6-7	6-7	7-8	7-8	7-8	8-9
18	4-5	5	5	5-6	6	6-7	6-7	d7-8	7-8	7-8
19	4	4-5	5	5	5-6	g6	6-7	6-7	6-8	7-8
20	4	4	4-5	n5	5	5-6	5-6	6A	6-7	6-7
21	3-4	4	4	4-5	4-5	5	5-6	5-6	6	6-7
22	3	3-4	4	4	4	4-5	5	5-6	5-6	6
23	3	3	3-4	4	4	4	4-5	5	5	5-6
24	g3	3	3	3-4	n4	4	4	4-5	5	5
25		2-3	3	3	3-4	3-4	4	4	4-5	5
26			2-3	3	3	3r	3-4	4	4	4-5
27				2-3	3	3	3r	3-4	4	4
28					2-3	3	3	3r	3-4	4
29						2-3	3	3	3	3-4
30							2C	3	3	3
31								2C	3	3
32									2r	3
33										2q

$k \setminus n$	43	44	45	46	47	48	49	50	51	52
6	d15-17	15-18	d16-18	16-19	16-19	17-20	17-20	f18-21	18-21	n19-22
7	14-17	14-17	n15-18	15-18	d16-19	16-19	16-20	17-20	17-21	d18-21
8	13-16	f14-17	14-17	14-18	n15-18	15-19	n16-19	16-20	16-20	17-21
9	12-15	13-16	13-16	f14-17	14-17	14-18	15-18	15-19	n16-19	16-20
10	12-15	12-15	12-16	13-16	13-17	n14-17	14-18	14-18	15-19	15-19
11	11-13	11-14	12-14	12-15	n13-15	13-16	13-16	14-17	14-17	f15-18
12	10-13	11-13	11-14	d12-14	12-15	12-15	13-16	13-16	13-17	14-17
13	10-12	10-13	n11-13	11-14	11-14	12-15	12-15	f13-16	13-16	13-17
14	9-11	10-12	10-12	g11-13	11-13	11-14	n12-14	12-15	12-15	n13-16
15	9-11	9-11	n10-12	10-12	10-13	n11-13	11-14	11-14	12-15	12-15
16	8-10	9-10	9-11	9-11	10-12	10-12	g11-12	11-13	11-13	n12-14
17	8-9	8-10	n9-10	9-11	9-11	10-12	10-12	10-12	11-13	11-13
18	7-9	8-9	8-10	8-10	9-11	9-11	9-12	10-12	10-12	d11-13
19	7-8	7-9	8-9	8-10	8-10	9-10A	9-11	9-11	10-12	10-12
20	7-8	7-8	7-9	8-9	8-9	8-10	n9-10	9-11	9-11	n10-12
21	6-7	7-8	7-8	7-9	n8-9	8-9	8-10	8-10	9-11	9-11
22	6-7	6-7	g7-8	7-8	7-9	7-9	8-9	8-10	8-10	9-10
23	n6	6	6	6-7	7	7-8	7-8	8-9	8-9	8-10
24	5-6	5-6	6	6	6-7	7	7-8	7-8	n8-9	8-9
25	5	5-6	5-6	6	6	6-7	7	7-8	7-8	g8-9
26	d5	5	5-6	5-6	6	6	6-7	n7	7	7-8
27	4-5	4-5	5	5-6	5-6	6	6	6-7	6-7	7
28	4	4-5	4-5	5	5-6	5-6	n6	6	6-7	6-7
29	4	4	4-5	4-5	5	5A	5-6	g6	6	6-7
30	3-4	4	4	4-5	4-5	5	5	5-6	5-6	6
31	3	3-4	4	4	4-5	4-5	5	5	5-6	5-6
32	3	3	3-4	4	4	4-5	4-5	5	5	5-6
33	3	3	3	3-4	3-4	4	4D	4-5	d5	5
34	2q	3	3	3	3-4	3-4	4	4C	4-5	d5
35			q3	3	3	3-4	3-4	4	4	4-5
36				d3	3	3	3-4	3-4	4	4
37					2-3	3	3	3-4	3-4	4
38						2-3	3	3	3-4	3-4
39							2-3	3	3	3-4
40								2-3	3	3
41									2-3	3
42										2-3

$k \backslash n$	53	54	55	56	57	58	59	60	61	62	63	64
6	19-22	19-23	20-23	20-24	f21-24	21-25	n22-25	22-26	g23-26	23-27	23-27	g24-28
7	18-22	18-22	19-23	19-23	d20-24	20-24	n21-25	21-25	21-26	22-26	22-27	g23-27
8	17-21	f18-22	18-22	18-23	19-23	19-24	d20-24	20-25	20-25	21-26	21-26	d22-27
9	16-20	17-21	17-21	n18-22	18-22	18-23	19-23	19-24	n20-24	20-25	20-25	21-26
10	n16-20	16-20	16-21	17-21	17-22	n18-22	18-23	18-23	19-24	19-24	n20-25	20-25
11	15-18	15-19	n16-19	16-20	16-20	17-21	17-21	n18-22	18-22	18-23	19-23	19-24
12	14-18	n15-18	15-19	15-19	16-20	16-20	n17-21	17-21	17-22	n18-22	18-23	18-23
13	n14-17	14-18	14-18	15-19	15-19	15-20	16-20	16-21	n17-21	17-22	17-22	18-23
14	13-16	13-17	14-17	14-18	14-18	15-19	15-19	d16-20	16-20	16-21	17-21	17-22
15	12-16	13-16	13-17	n14-17	14-18	14-18	n15-19	15-19	15-20	16-20	16-21	16-21
16	12-14	12-15	n13-15	13-16	13-16	14-17	14-17	14-18	15-18	15-19	n16-19	16-20
17	11-14	12-14	12-15	12-15	13-16	13-16	g14-17	14-17	14-18	n15-18	15-19	15-19
18	11-13	11-14	n12-14	12-15	12-15	n13-16	13-16	13-17	n14-17	14-18	14-18	15-19
19	10-13	11-13	11-13	11-14	12-14	12-15	12-15	13-16	13-16	g14-17	14-17	14-18
20	10-12	10-13	n11-13	11-13	11-14	d12-14	12-15	12-15	n13-16	13-16	13-17	14-17
21	9-12	10-12	10-13	10-13	11-13	11-14	11-14	12-14	12-14	12-15	13-15	13-16
22	9-10	9-11	10-11	10-12	10-12	11-13	11-13	11-14	12-14	12-14	12-15	13-15
23	9-10	9-10	9-11	n10-11	10-12	10-12	n11-13	11-13	11-14	n12-14	12-14	12-15
24	8-10	n9-10	9-10	9-11	9-11	10-12	10-12	10-13	11-13	11-14	11-14	12-14
25	8-9	8-10	8-10	9-10	9-11	9-11	10-11	10-12	10-12	11-13	11-13	11-14
26	7-8	8-9	8-9	8-10	9-10	9-11	9-11	n10-11	10-12	10-12	n11-13	11-13
27	7-8	7-8	8-9	8-9	8-10	n9-10	9-11	9-11	g10-11	10-12	10-12	10-13
28	7	7-8	7-8	n8-9	8-9	8-9	8-10	9-10	9-11	9-11	10-11	10-12
29	6-7	7	7-8	7-8	7-8	8-9	8-9	8-10	9-10	9-11	9-11	10-11
30	6-7	6-7	7	7-8	7-8	7-8	8-9	8-9	8-10	9-10	9-11	9-11
31	6	6-7	6-7	n7	7-8	7-8	7-8	8-9	8-9	8-9A	n9-10	9-10
32	5-6	6	6-7	6-7	6-7	7-8	7-8	7-8	8-9	8-9	8-9	8-10
33	5-6	5-6	6	6-7	6-7	6-7	7	7-8	7-8	d8-9	8-9	8-9
34	5	5-6	5-6	n6	6-7	6-7	6-7	7	7-8	7-8	7-8	8-9
35	4-5	5	5-6	5-6	5-6	6-7	6-7	6-7	7	7-8	7-8	7-8
36	4-5	4-5	5	5-6	5-6	5-6	6-7	6-7	6-7	d7	7-8	7-8
37	4	4-5	4-5	5	5-6	5-6	5-6	6A	6-7	6-7	6-7	7-8
38	4	4	4-5	4-5	5	5-6	5-6	5-6	6	6-7	6-7	6-7
39	3-4	4	4	4-5	4-5	5	5D	5-6	5-6	6	6-7	6-7
40	3A	3-4	4	4	4-5	4-5	5	5D	5-6	5-6	6	6-7
41	3	3	3-4	4	4	4-5	4-5	5	5	5-6	5-6	6
42	3	3	3	3-4	4	4	4-5	4-5	g5	5	5-6	5-6
43	2C	3	3	3	3-4	4	4	4-5	4-5	4-5	5	5-6
44		2C	3	3	3	3-4	d4	4	4-5	4-5	4-5	5
45			2C	3	3	3	3-4	3-4	4	4C	4-5	4-5
46				2C	3	3	3	3-4	3-4	4	4C	4-5
47					2C	3	3	3	3-4	3-4	4	4C
48						2q	3	3	3	3-4	3-4	4
49							2	3	3	3	3C	3-4
50								2	3	3	3	3C
51									2	3	3	3
52										2	3	3
53											2	r3
54												2

**Table C.** Table of lower and upper bounds for  $K_3(n, t)$ ,  $1 \leq n \leq 13, 1 \leq t \leq 3$ .

As often as possible, we mention the *earliest* reference.

**Key to Table C:**

unmarked = trivial.

p = perfect codes (let us mention that the  $(11, 729)t = 2$  code, often called a Golay code, was published as early as 1947 by J. Virtakallio, in a Finnish football pool magazine; see [84], [85] or [111]).

q = [135].

**lower bounds:**

s = sphere-covering bound.

b = [136].

c = stated without proof in [249]. The sphere-covering bound is 57, and 60 has been proved in [80].

d = [156].

e = [163].

f = [32].

g = [254].

h = [160].

i = [143].

j = [80].

**upper bounds:**

B = [17].

C = [145].

D = [85] (includes results previously published in football pool magazines).

E = [199].

F = [198].

$n$	$t = 1$	$t = 2$	$t = 3$
1	1		
2	3	1	
3	q 5 q	3	1
4	p 9 p	s 3	3
5	b 27	i 8 D	3
6	c 63–73 C	f 12–17 D	f 6 D
7	j 150–186 C	f 26–34 D	e 7–12 D
8	g 393–486 C	g 52–81 D	d 13–27 D
9	g 1048–1341 F	d 128–219 D	h 26–54 D
10	j 2818–3645 B	f 323–558 D	f 57–108 D
11	g 7767–9477 E	p 729 p	h 119–243 D
12	g 21395–27702 E	f 1919–2187	f 282–729
13	p 59049 p	f 5062–6561	f 609–1215 D

## References

- [1] E.H.L. AARTS and P.J.M. van LAARHOVEN: Local search in coding theory, *Discrete Mathematics*, vol. 106–107, pp. 11–18, 1992.
- [2] M.J. ADAMS: Subcodes and covering radius, *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 700–701, September 1986.
- [3] N. ALON and J. SPENCER: *The probabilistic method*, Wiley, 1992.
- [4] D.R. ANDERSON: A new class of cyclic codes, *SIAM Journal of Applied Mathematics*, vol. 16, pp. 181–197, 1968.
- [5] E.F. ASSMUS, Jr., and H.F. MATTSON, Jr.: Some 3-error correcting BCH codes have covering radius 5, *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 348–349, May 1976.
- [6] E.F. ASSMUS, Jr., and V.S. PLESS: On the covering radius of extremal self-dual codes, *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 359–363, May 1983.
- [7] A.M. BARG: At the dawn of the theory of codes, *Mathematical Intelligencer*, vol. 15, pp. 20–26, 1993.
- [8] J. BECK and T. FIALA: “Integer-making” theorems, *Discrete Applied Mathematics*, vol. 3, pp. 1–8, 1981.
- [9] E.R. BERLEKAMP and L.R. WELCH: Weight distribution of the cosets of the (32,6) Reed-Muller code, *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, January 1972.
- [10] M. BEVERAGGI and G.D. COHEN: On the density of best coverings in Hamming spaces, *Lecture Notes in Computer Science*, No. 311, pp. 39–44, Springer-Verlag, 1988.
- [11] M.C. BHANDARI and M.S. GARG: Comments on “On the covering radius of codes”, *IEEE Trans. Inform. Theory*, vol. 36, pp. 953–954, July 1990.
- [12] M.C. BHANDARI and M.S. GARG: A note on the covering radius of optimum codes, *Discrete Applied Mathematics*, vol. 33, pp. 3–9, 1991.
- [13] V.M. BLINOVSKII: Bounds for codes in the case of list decoding of finite volume, *Problemy Peredachi Informatsii*, vol. 22, pp. 11–25, 1986. Translated in: *Problems of Inform. Transm.*, vol. 22, No. 1, pp. 7–19, 1986.
- [14] V.M. BLINOVSKII: Lower asymptotic bound on the number of linear code words in a sphere of given radius in  $F_q^n$ , *Problemy Peredachi Informatsii*, vol. 23, pp. 50–53, 1987. Translated in: *Problems of Inform. Transm.*, vol. 23, No. 2, pp. 130–132, 1987.
- [15] V.M. BLINOVSKII: Asymptotically exact uniform bounds for spectra of cosets of linear codes, *Problemy Peredachi Informatsii*, vol. 26, pp. 99–103, 1990. Translated in: *Problems of Inform. Transm.*, vol. 26, No. 1, pp. 83–86, 1990.
- [16] V.M. BLINOVSKII: Covering the Hamming space with sets translated by linear code vectors, *Problemy Peredachi Informatsii*, vol. 26, pp. 21–26, 1990. Translated in: *Problems of Inform. Transm.*, vol. 26, No. 3, pp. 196–201, 1990.

- [17] A. BLOKHUIS and C.W.H. LAM: More coverings by rook domains, *Journal of Combinatorial Theory*, Ser. A, vol. 36, pp. 240–244, 1984.
- [18] A.E. BROUWER, J.B. SHEARER, N.J.A. SLOANE, and W.D. SMITH: A new table of constant weight codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 1334–1380, November 1990.
- [19] R.A. BRUALDI, N. CAI, and V.S. PLESS: Orphan structure of the first-order Reed-Muller codes, *Discrete Mathematics*, vol. 102, pp. 239–247, 1992.
- [20] R.A. BRUALDI and V.S. PLESS: Orphans of the first order Reed-Muller codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 399–401, March 1990.
- [21] R.A. BRUALDI and V.S. PLESS: On the covering radius of a code and its subcodes, *Discrete Mathematics*, vol. 83, pp. 189–199, 1990.
- [22] R.A. BRUALDI and V.S. PLESS: On the length of codes with a given covering radius. In: *Coding Theory and Design Theory. Part I: Coding Theory*, pp. 9–15, Springer-Verlag, 1990.
- [23] R.A. BRUALDI and V.S. PLESS: Covering radius. In: *Handbook of Coding Theory*, Eds. R.A. Brualdi, W.C. Huffman and V.S. Pless, to appear.
- [24] R.A. BRUALDI, V.S. PLESS, and R.M. WILSON: Short codes with a given covering radius, *IEEE Trans. Inform. Theory*, vol. 35, pp. 99–109, January 1989.
- [25] P.B. BUSSCHBACH, M.G.L. GERRETZEN, and H.C.A. van TILBORG: On the covering radius of binary linear codes meeting the Griesmer bound, *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 465–468, July 1985.
- [26] A.R. CALDERBANK: Covering radius and the chromatic number of Kneser graphs, *Journal of Combinatorial Theory*, Ser. A, vol. 54, pp. 129–131, 1990.
- [27] A.R. CALDERBANK: Covering bounds for codes, *Journal of Combinatorial Theory*, Ser. A, vol. 60, pp. 117–122, 1992.
- [28] A.R. CALDERBANK: Covering machines, *Discrete Mathematics*, vol. 106–107, pp. 105–110, 1992.
- [29] A.R. CALDERBANK and N.J.A. SLOANE: Inequalities for covering codes, *IEEE Trans. Inform. Theory*, vol. 34, pp. 1276–1280, September 1988.
- [30] W.A. CARNIELLI: On covering and coloring problems for rook domains, *Discrete Mathematics*, vol. 57, pp. 9–16, 1985.
- [31] W.A. CARNIELLI: Hyper-rook domain inequalities, *Stud. Appl. Math.*, vol. 82, pp. 59–69, 1990.
- [32] W. CHEN and I.S. HONKALA: Lower bounds for  $q$ -ary covering codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 664–671, May 1990.
- [33] V. CHVATAL: A greedy heuristic for the set-covering problem, *Mathematics of Operations Research*, vol. 4, pp. 233–235, 1979.



- [34] R.F. CLAYTON: Multiple packings and coverings in algebraic coding theory, Ph. D. Thesis, University of California in Los Angeles, United States, 62 p., 1987.
- [35] G.D. COHEN: A nonconstructive upper bound on covering radius, *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 352–353, May 1983.
- [36] G.D. COHEN: Non-linear covering codes: a few results and conjectures, *Lecture Notes in Computer Science*, No. 356, pp. 225–229, Springer-Verlag, 1989.
- [37] G.D. COHEN and P. FRANKL: On cliques and partitions in Hamming spaces, Rapport Interne ENST-C-81007, Ecole Nationale Supérieure des Télécommunications, Paris, 8 p., 1981.
- [38] G.D. COHEN and P. FRANKL: On generalized perfect codes and Steiner systems, *Annals of Discrete Mathematics*, vol. 18, pp. 197–200, 1983.
- [39] G.D. COHEN and P. FRANKL: Good coverings of Hamming spaces with spheres, *Discrete Mathematics*, vol. 56, pp. 125–131, 1985.
- [40] G.D. COHEN, Ph. GODLEWSKI, and F. MERKX: Linear binary codes for write-once memories, *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 697–700, September 1986.
- [41] G.D. COHEN, I.S. HONKALA, and S.N. LITSYN: On weighted coverings and packings with diameter one, *CISM Courses and Lectures*, No. 339, pp. 43–49, Springer-Verlag, 1993.
- [42] G.D. COHEN, I.S. HONKALA, S.N. LITSYN, and H.F. MATTSON, Jr.: Weighted coverings and packings, *IEEE Trans. Inform. Theory*, submitted.
- [43] G.D. COHEN, M.G. KARPOVSKY, H.F. MATTSON, Jr., and J.R. SCHATZ: Covering radius—survey and recent results, *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 328–343, May 1985.
- [44] G.D. COHEN and S.N. LITSYN: On the covering radius of Reed-Muller codes, *Discrete Mathematics*, vol. 106–107, pp. 147–155, 1992.
- [45] G.D. COHEN, S.N. LITSYN, and H.F. MATTSON, Jr.: On perfect weighted coverings with small radius, *Lecture Notes in Computer Science*, No. 573, pp. 32–41, Springer-Verlag, 1992.
- [46] G.D. COHEN, S.N. LITSYN, and H.F. MATTSON, Jr.: Binary perfect weighted coverings, I The linear case. In: *Sequences II*, Eds. Capocelli, DeSantis and Vaccaro, Springer-Verlag, pp. 36–51, 1993.
- [47] G.D. COHEN, A.C. LOBSTEIN, and N.J.A. SLOANE: Further results on the covering radius of codes, *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 680–694, September 1986.
- [48] G.D. COHEN, A.C. LOBSTEIN, and N.J.A. SLOANE: On a conjecture concerning coverings of Hamming space, *Lecture Notes in Computer Science*, No. 228, pp. 79–89, Springer-Verlag, 1986.
- [49] G.D. COHEN and G. ZÉMOR: An application of combinatorial group theory to coding, *Ars Combinatoria*, vol. 23-A, pp. 81–89, 1987.

- [50] A.A. DAVYDOV: Construction of linear covering codes, *Problemy Peredachi Informatsii*, vol. 26, pp. 38–55, 1990. Translated in: *Problems of Inform. Transm.*, vol. 26, No. 4, pp. 317–331, 1990.
- [51] A.A. DAVYDOV: Constructions of codes with covering radius 2, *Lecture Notes in Computer Science*, No. 573, pp. 23–31, Springer-Verlag, 1992.
- [52] A.A. DAVYDOV and A.Y. DROZHZHINA-LABINSKAYA: Binary linear codes with covering radii 3 and 4, 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory, Abstracts of papers, pp. 56–57, Leningrad, 1990.
- [53] A.A. DAVYDOV and A.Y. DROZHZHINA-LABINSKAYA: Table and families of short  $[n, n-r]$  codes with a given covering radius  $R$ , Preprint, 1990.
- [54] A.A. DAVYDOV and A.Y. DROZHZHINA-LABINSKAYA: Constructions of binary linear covering codes, Workshop on Algebraic and Combinatorial Coding Theory, Abstracts of papers, pp. 51–54, Voneshta Voda, 1992.
- [55] A.A. DAVYDOV and A.Y. DROZHZHINA-LABINSKAYA: Constructions, families and tables of binary linear covering codes, *IEEE Trans. Inform. Theory*, to appear.
- [56] P. DELIGNE: La conjecture de Weil I, Institut. Hautes Etudes Sci., *Publ. Math.*, vol. 43, pp. 273–307, 1974.
- [57] C. DELORME and P. SOLÉ: Diameter, covering index, covering radius and eigenvalues, *Europ. J. Combinatorics*, vol. 12, pp. 95–108, 1991.
- [58] P. DELSARTE: Four fundamental parameters of a code and their combinatorial significance, *Information and Control*, vol. 23, pp. 407–438, 1973.
- [59] P. DELSARTE and P. PIRET: Do most binary linear codes achieve the Gobleck bound on the covering radius?, *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 826–828, November 1986.
- [60] S.M. DODUNEKOV: Some quasi-perfect double error correcting codes, *Problems of Control and Information Theory*, vol. 15, No. 5, pp. 367–375, 1986.
- [61] S.M. DODUNEKOV, K.N. MANEV, and V.D. TONCHEV: On the covering radius of binary  $[14,6]$  codes containing the all-one vector, *IEEE Trans. Inform. Theory*, vol. 34, pp. 591–593, May 1988.
- [62] S.M. DODUNEKOV and N.L. MANEV: An improvement of the Griesmer bound for some small minimum distances, *Discrete Applied Mathematics*, vol. 12, pp. 103–114, 1985.
- [63] R. DOUGHERTY and H. JANWA: Covering radius computations for binary cyclic codes, *Mathematics of Computation*, vol. 57, pp. 415–434, July 1991.
- [64] D.E. DOWNIE and N.J.A. SLOANE: The covering radius of cyclic codes of length up to 31, *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 446–447, May 1985.
- [65] A.A. EL GAMAL, L.A. HAMACHANDRA, I. SHPERLING, and V.K. WEI: Using simulated annealing to design good codes, *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 116–123, January 1987.

- [66] M.H. EL-ZAHAR and M.K. KHAIRAT: On the weight distribution of the coset leaders of the first-order Reed-Muller code, *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 744–747, September 1987.
- [67] T. ETZION and G. GREENBERG: Constructions of perfect mixed codes and other covering codes, *IEEE Trans. Inform. Theory*, vol. 39, pp. 209–214, January 1993.
- [68] T. ETZION, G. GREENBERG, and I.S. HONKALA: Normal and abnormal codes, *IEEE Trans. Inform. Theory*, vol. 39, pp. 1453–1456, July 1993.
- [69] T. ETZION, V.K. WEI, and Z. ZHANG: Bounds on the sizes of constant weight covering codes, submitted.
- [70] G. FAZEKAS and V.I. LEVENSHTAIN: On upper bounds for code distance and covering radius of designs in polynomial metric spaces, *Proc. Fifth Joint Soviet-Swedish Workshop on Information Theory*, 1990.
- [71] M.R. FELLOWS: Encoding graphs in graphs, Ph. D. Thesis, University of California, San Diego, United States, 112 p., 1985.
- [72] H. FERNANDES and E. RECHTSCHAFFEN: The football pool problem for 7 and 8 matches, *Journal of Combinatorial Theory*, Ser. A, vol. 35, pp. 109–114, 1983.
- [73] P.C. FISHBURN and N.J.A. SLOANE: The solution to Berlekamp’s switching game, *Discrete Mathematics*, vol. 74, pp. 263–290, 1989.
- [74] M. FRANCES and A. LITMAN: On covering problems of codes, Technical Report No. 827, Technion, Haifa, Israel, 8 p., July 1994.
- [75] E.M. GABIDULIN, A.A. DAVYDOV, and L.M. TOMBAK: Linear codes with covering radius 2 and other new covering codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 219–224, January 1991.
- [76] A.M. GLEASON: Weight polynomials of self-dual codes and the MacWilliams identities, *Actes, Congrès Intern. Math.*, vol. 3, pp. 211–215, 1970.
- [77] Ph. GODLEWSKI: Wom-codes construits à partir des codes de Hamming, *Discrete Mathematics*, vol. 65, pp. 237–243, 1987.
- [78] D. GORENSTEIN, W.W. PETERSON, and N. ZIERLER: Two-error correcting Bose-Chaudhury codes are quasi-perfect, *Information and Control*, vol. 3, pp. 291–294, 1960.
- [79] R.L. GRAHAM and N.J.A. SLOANE: On the covering radius of codes, *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 385–401, May 1985.
- [80] L. HABSIEGER: Lower bounds for  $q$ -ary coverings by spheres of radius 1, *Journal of Combinatorial Theory*, Ser. A, vol. 67, pp. 199–222, 1994.
- [81] M.W. van der HAM: Simulated annealing applied in coding theory, Master’s Thesis, Eindhoven University of Technology, the Netherlands, 50 p., 1988.

- [82] H.O. HÄMÄLÄINEN, I.S. HONKALA, M.K. KAIKKONEN, and S.N. LITSYN: Bounds for binary multiple covering codes, *Designs, Codes and Cryptography*, vol. 3, No. 3, pp. 251–275, July 1993.
- [83] H.O. HÄMÄLÄINEN, I.S. HONKALA, S.N. LITSYN, and P.R.J. ÖSTERGARD: Bounds for binary codes that are multiple coverings of the farthest-off points, *SIAM Journal of Discrete Mathematics*, to appear.
- [84] H.O. HÄMÄLÄINEN, I.S. HONKALA, S.N. LITSYN, and P.R.J. ÖSTERGARD: Football pools—A game for mathematicians, *American Mathematical Monthly*, to appear.
- [85] H.O. HÄMÄLÄINEN and S. RANKINEN: Upper bounds for football pool problems and mixed covering codes, *Journal of Combinatorial Theory*, Ser. A, vol. 56, pp. 84–95, 1991.
- [86] P. HAMMOND:  $q$ -coverings, codes, and line graphs, *Journal of Combinatorial Theory*, Ser. B, vol. 30, pp. 32–35, 1981.
- [87] A. HARTMAN, W.H. MILLS, and R.C. MULLIN: Covering triples by quadruples: an asymptotic solution, *Journal of Combinatorial Theory*, Ser. A, vol. 41, pp. 117–138, 1986.
- [88] A. HARTMAN, R.C. MULLIN, and D.R. STINSON: Exact covering configurations and Steiner systems, *J. London Math. Soc.*, vol. 25, pp. 193–200, 1982.
- [89] O. HEDEN: A generalized Lloyd theorem and mixed perfect codes, Matematiska Institutionen Stockholms Universitet, Memorandum No. 8, 1974.
- [90] O. HEDEN: A new construction of group and nongroup perfect codes, *Information and Control*, vol. 34, pp. 314–323, 1977.
- [91] T. HELLESETH: All binary 3-errors correcting BCH codes of length  $2^m - 1$  have covering radius 5, *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 257–258, March 1978.
- [92] T. HELLESETH: On the covering radius of cyclic linear codes and arithmetic codes, *Discrete Applied Mathematics*, vol. 11, pp. 157–173, 1985.
- [93] T. HELLESETH, T. KLOVE, and J. MYKKELTVEIT: On the covering radius of binary codes, *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 627–628, September 1978.
- [94] T. HELLESETH and H.F. MATTSON, Jr.: On the cosets of the simplex code, *Discrete Mathematics*, vol. 56, pp. 169–189, 1985.
- [95] M. HERZOG and J. SCHÖNHEIM: Linear and nonlinear single-error correcting perfect mixed codes, *Information and Control*, vol. 18, pp. 364–368, 1971.
- [96] M. HERZOG and J. SCHÖNHEIM: Group partition, factorization and the vector covering problem, *Canad. Math. Bull.*, vol. 15, pp. 207–214, 1972.
- [97] I.S. HONKALA: On the intersections and unions of Hamming spheres. In: *The Very Knowledge of Coding*, Turku, Finland, pp. 70–81, 1987.
- [98] I.S. HONKALA: Bounds for binary constant weight and covering codes, Licentiate Thesis, University of Turku, Finland, 75 p., 1987.

- [99] I.S. HONKALA: Lower bounds for binary covering codes, *IEEE Trans. Inform. Theory*, vol. 34, pp. 326–329, March 1988.
- [100] I.S. HONKALA: Combinatorial bounds for binary constant weight and covering codes, Ph. D. Thesis, University of Turku, Finland, 108 p., January 1989.
- [101] I.S. HONKALA: On the normality of codes with covering radius one, *Proc. Fourth Joint Swedish-Soviet Workshop on Information Theory*, pp. 223–226, 1989.
- [102] I.S. HONKALA: Modified bounds for covering codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 351–365, March 1991.
- [103] I.S. HONKALA: On  $(k, t)$ -subnormal covering codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 1203–1206, July 1991.
- [104] I.S. HONKALA: All binary codes with covering radius one are subnormal, *Discrete Mathematics*, vol. 94, pp. 229–232, 1991.
- [105] I.S. HONKALA: On lengthening of covering codes, *Discrete Mathematics*, vol. 106–107, pp. 291–295, 1992.
- [106] I.S. HONKALA: A Graham-Sloane type construction for  $s$ -surjective matrices, *Journal of Algebraic Combinatorics*, vol. 1, pp. 347–351, 1992.
- [107] I.S. HONKALA: A lower bound on binary codes with covering radius one, *Lecture Notes in Computer Science*, No. 781, pp. 34–37, Springer-Verlag, 1994.
- [108] I.S. HONKALA: On the normality of multiple covering codes, *Discrete Mathematics*, vol. 125, pp. 229–239, 1994.
- [109] I.S. HONKALA: On  $(q, 1)$ -subnormal  $q$ -ary covering codes, *Discrete Applied Mathematics*, vol. 152, pp. 213–221, 1994.
- [110] I.S. HONKALA: A new lower bound on codes with covering radius one, *ISITA '94*, to appear.
- [111] I.S. HONKALA: On the early history of the ternary Golay code, Unpublished.
- [112] I.S. HONKALA and H.O. HÄMÄLÄINEN: A new construction for covering codes, *IEEE Trans. Inform. Theory*, vol. 34, pp. 1343–1344, September 1988.
- [113] I.S. HONKALA and H.O. HÄMÄLÄINEN: Bounds for abnormal binary codes with covering radius one, *IEEE Trans. Inform. Theory*, vol. 37, pp. 372–375, March 1991.
- [114] I.S. HONKALA, Y. KAIPAINEN, and A. TIETÄVÄINEN: Long binary narrow-sense BCH codes are normal, *Applicable Algebra in Engineering, Communication and Computing*, submitted.
- [115] I.S. HONKALA and S.N. LITSYN: Generalizations of the covering radius problem in coding theory, *Proc. Jerusalem Combinatorics 1993*, submitted.
- [116] I.S. HONKALA and P.R.J. ÖSTERGARD: Applications in code design. In: *Local Search in Combinatorial Optimization*, Chapter 12, Eds. E.H.L. Aarts and J.K. Lenstra, to appear.

- [117] I.S. HONKALA and A. TIETÄVÄINEN: Codes and number theory. In: *Handbook of Coding Theory*, Eds. R.A. Brualdi, W.C. Huffman and V.S. Pless, to appear.
- [118] J.A. van der HORST and T. BERGER: Complete decoding of triple-error-correcting binary BCH codes, *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 138–147, March 1976.
- [119] X.D. HOU: Covering radius and error correcting codes, Ph. D. Thesis, University of Illinois, Chicago, United States, 77 p., 1990.
- [120] X.D. HOU: Some results on the norm of codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 683–685, May 1990.
- [121] X.D. HOU: New lower bounds for covering codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 895–899, July 1990.
- [122] X.D. HOU: An improved sphere covering bound for the codes with  $n = 3R + 2$ , *IEEE Trans. Inform. Theory*, vol. 36, pp. 1476–1478, November 1990.
- [123] X.D. HOU: Binary linear quasi-perfect codes are normal, *IEEE Trans. Inform. Theory*, vol. 37, pp. 378–379, March 1991.
- [124] X.D. HOU: On the covering radius of subcodes of a code, *IEEE Trans. Inform. Theory*, vol. 37, pp. 1706–1707, November 1991.
- [125] X.D. HOU: Some results on the covering radii of Reed-Muller codes, *IEEE Trans. Inform. Theory*, vol. 39, pp. 366–378, March 1993.
- [126] X.D. HOU: Further results on the covering radii of the Reed-Muller codes, *Designs, Codes and Cryptography*, vol. 3, No. 2, pp. 167–177, May 1993.
- [127] X.D. HOU: The Reed-Muller code  $R(1, 7)$  is normal, to appear.
- [128] H. JANWA: Relations among parameters of codes, Ph. D. Thesis, Syracuse University, United States, 116 p., 1986.
- [129] H. JANWA: Some new upper bounds on the covering radius of binary linear codes, *IEEE Trans. Inform. Theory*, vol. 35, pp. 110–122, January 1989.
- [130] H. JANWA: Some optimal codes from algebraic geometry and their covering radii, *Europ. J. Combinatorics*, vol. 11, pp. 249–266, 1990.
- [131] H. JANWA: On the parameters of algebraic geometric codes, *Lecture Notes in Computer Science*, No. 539, pp. 19–28, Springer-Verlag, 1991.
- [132] H. JANWA and H.F. MATTSON, Jr.: Covering radii of even subcodes of  $t$ -dense codes, *Lecture Notes in Computer Science*, No. 229, pp. 120–130, Springer-Verlag, 1986.
- [133] H. JANWA and H.F. MATTSON, Jr.: On the normality of binary linear codes, *IEEE Trans. Inform. Theory*, submitted.

- [134] G.A. KABATIANSKII and V.I. PANCHENKO: Unit sphere packings and coverings of the Hamming space, *Problemy Peredachi Informatsii*, vol. 24, pp. 3–16, 1988. Translated in: *Problems of Inform. Transm.*, vol. 24, No. 4, pp. 261–272, 1988.
- [135] J.G. KALBFLEISCH and R.G. STANTON: A combinatorial problem in matching, *J. London Math. Soc.*, vol. 44, pp. 60–64, 1969.
- [136] H.J.L. KAMPS and J.H. van LINT: The football pool problem for 5 matches, *Journal of Combinatorial Theory*, Ser. A, vol. 3, pp. 315–325, 1967.
- [137] H.J.L. KAMPS and J.H. van LINT: A covering problem, *Colloquia Mathematica Societatis János Bolyai*, vol. 4, pp. 679–685, 1970.
- [138] G.L. KATSMAN: Bounds on covering radius of dual product codes, *Lecture Notes in Computer Science*, No. 573, pp. 52–57, Springer-Verlag, 1992.
- [139] K.E. KILBY and N.J.A. SLOANE: On the covering radius problem for codes: I Bounds on normalized covering radius, II Codes of low dimension; normal and abnormal codes, *SIAM Journal of Algebraic and Discrete Methods*, vol. 8, pp. 604–627, 1987.
- [140] S. KIRKPATRICK, C.D. GELATT, Jr., and M.P. VECCHI: Optimization by simulated annealing, *Science*, vol. 220, pp. 671–680, May 1983.
- [141] D.J. KLEITMAN: On a combinatorial conjecture of Erdős, *Journal of Combinatorial Theory*, vol. 1, pp. 209–214, 1966.
- [142] E. KOLEV: Codes over GF(3) of length 5, 27 codewords and covering radius 1, submitted.
- [143] E. KOLEV and I. LANDGEV: On some mixed covering codes of small length, *Lecture Notes in Computer Science*, No. 781, pp. 38–50, Springer-Verlag, 1994.
- [144] K.U. KOSCHNICK: A new upper bound for the football pool problem for nine matches, *Journal of Combinatorial Theory*, Ser. A, vol. 62, pp. 162–167, 1993.
- [145] P.J.M. van LAARHOVEN, E.H.L. AARTS, J.H. van LINT, and L.T. WILLE: New upper bounds for the football pool problem for 6, 7 and 8 matches, *Journal of Combinatorial Theory*, Ser. A, vol. 52, pp. 304–312, 1989.
- [146] J.M. LABORDE: Une nouvelle famille de codes binaires, parfaits, non linéaires, *Comptes-Rendus de l'Académie des Sciences*, Ser. I, vol. 297, pp. 67–70, 1983.
- [147] J.M. LABORDE: Sur le nombre domatique du  $n$ -cube et une conjecture de Zelinka, *Europ. J. Combinatorics*, vol. 8, pp. 175–177, 1987.
- [148] J. LAHTONEN: An optimal polynomial for a covering radius problem, *Discrete Mathematics*, vol. 105, pp. 313–317, 1992.
- [149] S. LANG and A. WEIL: Number of points of varieties in finite fields, *American Journal of Mathematics*, vol. 76, pp. 819–827, 1954.
- [150] P. LANGEVIN: The covering radius of RM(1,9) into RM(3,9), *Lecture Notes in Computer Science*, No. 514, pp. 51–59, Springer-Verlag, 1991.

- [151] H.W. LENSTRA, Jr.: Two theorems on perfect codes, *Discrete Mathematics*, vol. 3, pp. 125–132, 1972.
- [152] D. LI and W. CHEN: New lower bounds for binary covering codes, *IEEE Trans. Inform. Theory*, to appear.
- [153] B. LINDSTRÖM: Group partitions and mixed perfect codes, *Canad. Math. Bull.*, vol. 18, pp. 57–60, 1975.
- [154] J.H. van LINT: A survey of perfect codes, *Rocky Mountain J. Math.*, vol. 5, pp. 199–224, 1975.
- [155] J.H. van LINT: Recent results on covering problems, *Lecture Notes in Computer Science*, No. 357, pp. 7–21, Springer-Verlag, 1989.
- [156] J.H. van LINT, Jr.: Covering radius problems, Master’s Thesis, Eindhoven University of Technology, the Netherlands, 41 p., 1988.
- [157] J.H. van LINT, Jr., and G.J.M. van WEE: Generalized bounds on binary-ternary mixed packing and covering codes, *Journal of Combinatorial Theory*, Ser. A, vol. 57, pp. 130–143, 1991.
- [158] S.N. LITSYN, C.J. MORENO, and O. MORENO: Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables, *Applicable Algebra in Engineering, Communication and Computing*, vol. 5, pp. 105–116, 1994.
- [159] S.N. LITSYN, P. SOLÉ, and A. TIETÄVÄINEN: Covering radius, dual distance and codimension, in preparation.
- [160] C. LO and Z. ZHANG: New lower bounds for  $K_3(n, R)$  from linear inequalities, *IEEE Trans. Inform. Theory*, submitted.
- [161] A.C. LOBSTEIN, G.D. COHEN, and N.J.A. SLOANE: Recouvrements d’espaces de Hamming binaires, *Comptes-Rendus de l’Académie des Sciences*, Ser. I, vol. 301, pp. 135–138, 1985.
- [162] A. LOBSTEIN and V.S. PLESS: The length function: a revised table, *Lecture Notes in Computer Science*, No. 781, pp. 51–55, Springer-Verlag, 1994.
- [163] A.C. LOBSTEIN and G.J.M. van WEE: On normal and subnormal  $q$ -ary codes, *IEEE Trans. Inform. Theory*, vol. 35, pp. 1291–1295, November 1989, and vol. 36, p. 1498, November 1990.
- [164] L. LOVASZ: On the ratio of optimal integral and fractional covers, *Discrete Mathematics*, vol. 13, pp. 383–390, 1975.
- [165] L. LOVASZ: Covers, packings, and some heuristic algorithms, *Proc. 5th British Combinatorial Conf.*, pp. 417–429, 1975.
- [166] F.J. MACWILLIAMS and N.J.A. SLOANE: *The theory of error-correcting codes*, Amsterdam, The Netherlands: North-Holland, 1977.



- [167] J.A. MAIORANA: A classification of the cosets of the Reed-Muller code  $R(1, 6)$ , *Mathematics of Computation*, vol. 57, pp. 403–414, July 1991.
- [168] H.F. MATTSON, Jr.: An upper bound on covering radius, *Annals of Discrete Mathematics*, vol. 17, pp. 453–458, 1982.
- [169] H.F. MATTSON, Jr.: Another upper bound on covering radius, *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 356–359, May 1983.
- [170] H.F. MATTSON, Jr.: An improved upper bound on covering radius, *Lecture Notes in Computer Science*, No. 228, pp. 90–106, Springer-Verlag, 1986.
- [171] H.F. MATTSON, Jr.: Simplifications to “A new approach to the covering radius...”, *Journal of Combinatorial Theory*, Ser. A, vol. 57, pp. 311–315, July 1991.
- [172] H.F. MATTSON, Jr., and J.R. SCHATZ: A brief survey of covering radius, *Annals of Discrete Mathematics*, vol. 18, pp. 617–624, 1983.
- [173] J.G. MAULDON: Covering theorems for groups, *Quart. J. Math. Oxford*, vol. 1, pp. 284–287, 1950.
- [174] A. MCLOUGHLIN: The covering radius of the  $(m-3)$ rd order Reed-Muller codes and a lower bound on the  $(m-4)$ th order Reed-Muller codes, *SIAM Journal of Applied Mathematics*, vol. 37, pp. 419–422, 1979.
- [175] A. MCLOUGHLIN: The complexity of computing the covering radius of a code, *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 800–804, November 1984.
- [176] W.H. MILLS: Covering designs I: Coverings by a small number of subsets, *Ars Combinatoria*, vol. 8, pp. 199–315, 1979.
- [177] M. MOLLARD: Les invariants du  $n$ -cube, Thèse de 3ème cycle, Université de Grenoble, France, 113 p., 1981.
- [178] M. MOLLARD: Une nouvelle famille de 3-codes parfaits sur  $GF(q)$ , *Discrete Mathematics*, vol. 49, pp. 209–212, 1984.
- [179] M. MOLLARD: A generalized parity function and its use in the construction of perfect codes, *SIAM Journal of Algebraic and Discrete Methods*, vol. 7, pp. 113–115, 1986.
- [180] C.J. MORENO and O. MORENO: Exponential sums and Goppa codes I, *Proc. American Math. Soc.*, vol. 111, pp. 523–531, 1991.
- [181] C.J. MORENO and O. MORENO: Exponential sums and Goppa codes II, *IEEE Trans. Inform. Theory*, vol. 38, pp. 1222–1229, July 1992.
- [182] O. MORENO: Personal communication, 1992.
- [183] O. MORENO and C.J. MORENO: Constructive elementary approach to the covering radius of long BCH codes, 2nd Internat. Workshop on Algebraic and Combinatorial Coding Theory, Abstracts of papers, pp. 162–165, Leningrad, 1990.

- [184] O. MORENO and C.J. MORENO: Constructive elementary approach to the covering radius of long BCH codes, Preprint.
- [185] J. MYKKELTVEIT: The covering radius of the (128,8) Reed-Muller code is 56, *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 359–362, May 1980.
- [186] K.J. NURMELA: Constructing combinatorial designs by local search, J. Sc. Thesis, Helsinki University of Technology, Research Report, Series A, No. 27, 76 p., November 1993.
- [187] K.J. NURMELA and P.R.J. ÖSTERGARD: Constructing covering designs by simulated annealing, Helsinki University of Technology, Technical Report, Series B, No. 10, 25 p., January 1993.
- [188] K.J. NURMELA and P.R.J. ÖSTERGARD: Upper bounds for covering designs by simulated annealing, *Congressus Numerantium*, to appear.
- [189] J.E. OLSON and J. SPENCER: Balancing families of sets, *Journal of Combinatorial Theory*, Ser. A, vol. 25, pp. 29–37, 1978.
- [190] P.R.J. ÖSTERGARD: A new binary code of length 10 and covering radius 1, *IEEE Trans. Inform. Theory*, vol. 37, pp. 179–180, January 1991.
- [191] P.R.J. ÖSTERGARD: Upper bounds for  $q$ -ary covering codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 660–664, May 1991, and vol. 37, p. 1738, November 1991.
- [192] P.R.J. ÖSTERGARD: Constructions of mixed covering codes, Helsinki University of Technology, Research Report, Series A, No. 18, 44 p., December 1991.
- [193] P.R.J. ÖSTERGARD: Further results on  $(k, t)$ -subnormal covering codes, *IEEE Trans. Inform. Theory*, vol. 38, pp. 206–210, January 1992.
- [194] P.R.J. ÖSTERGARD: Construction methods for covering codes, Ph. D. Thesis, Helsinki University of Technology, Research Report, Series A, No. 25, 107 p., September 1993.
- [195] P.R.J. ÖSTERGARD: New upper bounds for the football pool problem for 11 and 12 matches, *Journal of Combinatorial Theory*, Ser. A, vol. 67, pp. 161–168, 1994.
- [196] P.R.J. ÖSTERGARD: Construction methods for mixed covering codes, *Proc. 21st Nordic Congress of Mathematicians*, M. Dekker, New York, to appear.
- [197] P.R.J. ÖSTERGARD: New constructions for  $q$ -ary covering codes, *Discrete Mathematics*, submitted.
- [198] P.R.J. ÖSTERGARD: Constructing covering codes by tabu search, *Discrete Applied Mathematics*, submitted.
- [199] P.R.J. ÖSTERGARD and H.O. HÄMÄLÄINEN: New upper bounds for binary-ternary mixed covering codes, Helsinki University of Technology, Research Report, Series A, No. 22, 33 p., March 1993.
- [200] P.R.J. ÖSTERGARD and H.O. HÄMÄLÄINEN: A new table of binary-ternary mixed covering codes, *Designs, Codes and Cryptography*, submitted.

- [201] J. PACH and J. SPENCER: Explicit codes with low covering radius, *IEEE Trans. Inform. Theory*, vol 34, pp. 1281–1285, September 1988.
- [202] V.I. PANCHENKO: Packings and coverings over an arbitrary alphabet, *Problemy Peredachi Informatsii*, vol. 24, pp. 93–96, 1988. Translated in: *Problems of Inform. Transm.*, vol. 24, No. 4, pp. 331–333, 1988.
- [203] N.J. PATTERSON and D.H. WIEDEMANN: The covering radius of the  $(2^{15}, 16)$  Reed-Muller code is at least 16276, *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 354–356, May 1983.
- [204] N.J. PATTERSON and D.H. WIEDEMANN: Correction to “The covering radius of the  $(2^{15}, 16)$  Reed-Muller code is at least 16276”, *IEEE Trans. Inform. Theory*, vol. 36, p. 443, March 1990.
- [205] K.T. PHELPS: A combinatorial construction of perfect codes, *SIAM Journal of Algebraic and Discrete Methods*, vol. 4, pp. 398–403, 1983.
- [206] K.T. PHELPS: A general product construction for error correcting codes, *SIAM Journal of Algebraic and Discrete Methods*, vol. 5, pp. 224–228, 1984.
- [207] K.T. PHELPS: Dual product constructions of Reed-Muller type codes, *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 103–106, January 1986.
- [208] H.F.H. REUVERS: Some non-existence theorems for perfect codes over arbitrary alphabets, Thesis, Eindhoven University of Technology, the Netherlands, 1977.
- [209] R.L. RIVEST and A. SHAMIR: How to reuse a “write-once” memory, *Information and Control*, vol. 55, pp. 1–19, 1982.
- [210] E.R. RODEMICH: Coverings by rook domains, *Journal of Combinatorial Theory*, Ser. A, vol. 9, pp. 117–128, 1970.
- [211] V. RÖDL: On a packing and covering problem, *Europ. J. Combinatorics*, vol. 5, pp. 69–78, 1985.
- [212] O. ROTHHAUS: On “bent” functions, *Journal of Combinatorial Theory*, Ser. A, vol. 20, pp. 300–305, 1976.
- [213] J.A. RUSH: Thin lattice coverings, *J. London Math. Soc.* (2), vol. 45, pp. 193–200, 1992.
- [214] J.R. SCHATZ: The second order Reed-Muller code of length 64 has covering radius 18, *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 529–530, July 1981.
- [215] J. SCHÖNHEIM: A new perfect single-error-correcting group code. Mixed codes, *Combinatorial Structures and Their Applications*, Gordon and Breach, London, p. 385, 1970.
- [216] J. SIMONIS: The minimal covering radius  $t[15, 6]$  of a 6-dimensional binary linear code of length 15 is equal to 4, *IEEE Trans. Inform. Theory*, vol. 34, pp. 1344–1345, September 1988.
- [217] J. SIMONIS: Covering radius: improving on the sphere-covering bound, *Lecture Notes in Computer Science*, No. 357, pp. 377–385, Springer-Verlag, 1989.

- [218] A.N. SKOROBOGATOV: On the covering radius of BCH codes, Third Internat. Workshop on Information Theory, Abstracts of papers, pp. 308–309, Sochi, 1987.
- [219] A.N. SKOROBOGATOV: The parameters of subcodes of algebraic-geometric codes over prime subfields, *Discrete Applied Mathematics*, vol. 33, pp. 205–214, 1991.
- [220] N.J.A. SLOANE: A new approach to the covering radius of codes, *Journal of Combinatorial Theory*, Ser. A, vol. 42, pp. 61–86, 1986.
- [221] N.J.A. SLOANE: Unsolved problems related to the covering radius of codes. In: *Open Problems in Communication and Computation*, pp. 51–56, Springer-Verlag, 1987.
- [222] N.J.A. SLOANE and R.J. DICK: On the enumeration of cosets of first order Reed-Muller codes, *Proc. IEEE Internat. Conf. Communications*, vol. 7, pp. 362–366, 1971.
- [223] P. SOLÉ: Asymptotic bounds on the covering radius of binary codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 1470–1472, November 1990.
- [224] P. SOLÉ: Covering codes and combinatorial optimization, *Lecture Notes in Computer Science*, No. 539, pp. 426–433, Springer-Verlag, 1991.
- [225] P. SOLÉ and K.G. MEHROTRA: Generalization of the Norse bounds to codes of higher strength, *IEEE Trans. Inform. Theory*, vol. 37, pp. 190–192, January 1991.
- [226] P. SOLÉ and Ph. STOKES: Covering radius, codimension and dual-distance width, *IEEE Trans. Inform. Theory*, vol. 39, pp. 1195–1203, July 1993.
- [227] P. SOLÉ and T. ZASLAVSKY: The covering radius of the cycle code of a graph, *Discrete Applied Mathematics*, vol. 45, pp. 63–70, 1993.
- [228] R.G. STANTON: Covering theorems in groups (or: how to win at football pools). In: *Recent Progress in Combinatorics*, pp. 21–36, Academic Press, New York, 1969.
- [229] R.G. STANTON, J.D. HORTON, and J.G. KALBFLEISCH: Covering theorems for vectors with special reference to the case of four and five components, *J. London Math. Soc.*, vol. 1, pp. 493–499, 1969.
- [230] R.G. STANTON and J.G. KALBFLEISCH: Covering problems for dichotomized matchings, *Aequationes Math.*, vol. 1, pp. 94–103, 1968.
- [231] R.G. STANTON and J.G. KALBFLEISCH: Intersection inequalities for the covering problem, *SIAM Journal of Applied Mathematics*, vol. 17, pp. 1311–1316, November 1969.
- [232] R. STRUIK: Constructive non-existence proofs for covering codes, Presented at Oberwolfach Workshop on Inform. Theory, April 1992.
- [233] R. STRUIK: Constructive non-existence proofs for linear covering codes, IEEE Symposium on Inform. Theory, Abstracts of papers, p. 369, San Antonio, January 1993.
- [234] R. STRUIK: An improvement of the van Wee bound for linear covering codes, *IEEE Trans. Inform. Theory*, vol. 40, July 1994.

- [235] R. STRUIK: On the structure of linear codes with covering radius two and three, *IEEE Trans. Inform. Theory*, vol. 40, September 1994.
- [236] R. STRUIK: Covering codes, Ph. D. Thesis, Eindhoven University of Technology, the Netherlands, 106 p., 1994.
- [237] O. TAUSKY and J. TODD: Covering theorems for groups, *Annales Soc. Polonaise de Math.*, vol. 21, pp. 303–305, 1948.
- [238] A. TIETÄVÄINEN: On the covering radius of long binary BCH codes, *Discrete Applied Mathematics*, vol. 16, pp. 75–77, 1987.
- [239] A. TIETÄVÄINEN: Codes and character sums, *Lecture Notes in Computer Science*, No. 388, pp. 3–12, Springer-Verlag, 1989.
- [240] A. TIETÄVÄINEN: An asymptotic bound on the covering radii of binary BCH codes, *IEEE Trans. Inform. Theory*, vol. 36, pp. 211–213, January 1990.
- [241] A. TIETÄVÄINEN: An upper bound on the covering radius as a function of the dual distance, *IEEE Trans. Inform. Theory*, vol. 36, pp. 1472–1474, November 1990.
- [242] A. TIETÄVÄINEN: Covering radius and dual distance, *Designs, Codes and Cryptography*, vol. 1, No. 1, pp. 31–46, May 1991.
- [243] H.C.A. van TILBORG: On the uniqueness (resp. nonexistence) of certain codes meeting the Griesmer bound, *Information and Control*, vol. 44, pp. 16–35, 1980.
- [244] M. TSFASMAN and S.G. VLEDUTS: *Algebraic-geometric codes*, Kluwer, Boston, 1991.
- [245] R.J.M. VAESSENS, E.H.L. AARTS, and J.H. van LINT: Genetic algorithms in coding theory—A table for  $A_3(n, d)$ , *Discrete Applied Mathematics*, vol. 45, pp. 71–87, 1993.
- [246] E. VELIKOVA: Bounds on the covering radius of linear codes, *Comptes-Rendus de l'Académie Bulgare des Sciences*, vol. 41, pp. 13–16, 1988.
- [247] E. VELIKOVA: Covering radius of some cyclic codes, Internat. Workshop on Algebraic and Combinatorial Coding Theory, Abstracts of papers, pp. 165–169, Varna, 1988.
- [248] S.G. VLEDUTS and A.N. SKOROBOGATOV: Covering radius for long BCH codes, *Problemy Peredachi Informatsii*, vol. 25, pp. 38–45, 1989. Translated in: *Problems of Inform. Transm.*, vol. 25, No. 1, pp. 28–34, 1989.
- [249] E.W. WEBER: On the football pool problem for 6 matches: a new upper bound, *Journal of Combinatorial Theory*, Ser. A, vol. 35, pp. 106–108, 1983.
- [250] G.J.M. van WEE: Improved sphere bounds on the covering radius of codes, *IEEE Trans. Inform. Theory*, vol. 34, pp. 237–245, March 1988.
- [251] G.J.M. van WEE: More binary covering codes are normal, *IEEE Trans. Inform. Theory*, vol. 36, pp. 1466–1470, November 1990.

- [252] G.J.M. van WEE: On the non-existence of certain perfect mixed codes, *Discrete Mathematics*, vol. 87, pp. 323–326, 1991.
- [253] G.J.M. van WEE: Bounds on packings and coverings by spheres in  $q$ -ary and mixed Hamming spaces, *Journal of Combinatorial Theory*, Ser. A, vol. 57, pp. 117–129, 1991.
- [254] G.J.M. van WEE: Some new lower bounds for binary and ternary covering codes, *IEEE Trans. Inform. Theory*, vol. 39, pp. 1422–1424, July 1993.
- [255] G.J.M. van WEE, G.D. COHEN, and S.N. LITSYN: A note on perfect multiple coverings of the Hamming space, *IEEE Trans. Inform. Theory*, vol. 37, pp. 678–682, May 1991.
- [256] L.T. WILLE: The football pool problem for 6 matches: a new upper bound obtained by simulated annealing, *Journal of Combinatorial Theory*, Ser. A, vol. 45, pp. 171–177, 1987.
- [257] L.T. WILLE: Personal communication, 1987.
- [258] L.T. WILLE: Improved binary code coverings by simulated annealing, *Congressus Numerantium*, vol. 73, pp. 53–58, January 1990.
- [259] Ø. YTREHUS: Binary  $[18,11]_2$  codes do not exist—nor do  $[64,53]_2$  codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 349–351, March 1991.
- [260] S.K. ZAREMBA, A covering theorem for abelian groups, *J. London Math. Soc.*, vol. 26, pp. 71–72, 1950.
- [261] S.K. ZAREMBA, Covering problems concerning abelian groups, *J. London Math. Soc.*, vol. 27, pp. 242–246, 1952.
- [262] B. ZELINKA: Domatic numbers of cube graphs, *Math. Slovaca*, vol. 32, pp. 117–119, 1982.
- [263] G. ZÉMOR: Problèmes combinatoires liés à l’écriture sur des mémoires, Thèse, Télécom Paris, France, 109 p., 1989.
- [264] G. ZÉMOR and G.D. COHEN: Error-correcting WOM-codes, *IEEE Trans. Inform. Theory*, vol. 37, pp. 730–734, May 1991.
- [265] Z. ZHANG: Linear inequalities for covering codes: Part I—pair covering inequalities, *IEEE Trans. Inform. Theory*, vol. 37, pp. 573–582, May 1991.
- [266] Z. ZHANG and C. LO: Linear inequalities for covering codes: Part II—triple covering inequalities, *IEEE Trans. Inform. Theory*, vol. 38, pp. 1648–1662, November 1992.
- [267] Z. ZHANG and C. LO: Lower bounds on  $t[n, k]$  from linear inequalities, *IEEE Trans. Inform. Theory*, vol. 38, pp. 194–197, January 1992.