HELSINKI UNIVERSITY OF TECHNOLOGY
DIGITAL SYSTEMS LABORATORY
Series **A:** Research Reports
No. **25**; September 1993
ISSN 0783–5396
ISBN 951–22–1696–5

CONSTRUCTION METHODS FOR COVERING CODES

Patric R. J. Östergård

Digital Systems Laboratory
Department of Computer Science
Helsinki University of Technology
SF–02150 Espoo, Finland

Helsinki University of Technology
Department of Computer Science
Digital Systems Laboratory
Otaniemi, Otakaari 1
SF–02150 ESPOO, FINLAND

HELSINKI UNIVERSITY OF TECHNOLOGY
DIGITAL SYSTEMS LABORATORY
Series **A:** Research Reports
No. **25**; September 1993

ISSN 0783–5396
ISBN 951–22–1696–5

Construction Methods for Covering Codes

PATRIC R. J. ÖSTERGÅRD

Abstract: A covering code in a Hamming space is a set of codewords with the property that any word in the space is within a specified Hamming distance, the covering radius, from at least one codeword. In this thesis, efficient construction methods for such codes are considered. The constructions work, with some exceptions, for codes over alphabets consisting of any number of symbols. Codes over mixed alphabets are also discussed. Most of the methods are developed in order to determine values of $K_q(n, R)$, the minimum number of codewords in a q-ary code of length n and covering radius R. Codes obtained by the constructions prove upper bounds on this function.

In many of the constructions simulated annealing, a probabilistic optimization method, has turned out to perform very well. Simulated annealing cannot be used to prove optimality of codes found; in that case, the problem is viewed and solved as a set covering problem. For larger codes, a direct approach is not generally feasible; it is shown how good such codes can be found by combining existing codes, or by imposing some structure on the codes. A matrix method that is presented follows the latter principle; a code constructed by this method consists of cosets of a linear code. To be able to combine existing codes efficiently, it is necessary that the codes involved can be partitioned into subcodes with certain properties; subnorm and norm are concepts that are introduced to describe partitions of codes. Finally, some families of combinatorial methods are presented.

Keywords: Combinatorial optimization, code construction, covering code, covering radius, football pool problem, simulated annealing.

Dissertation for the degree of Doctor of Technology to be presented with due permission for public examination and debate in Auditorium L at Helsinki University of Technology (Espoo, Finland) on the 10th of September, 1993, at 12 o'clock noon.

Printing: TKK Monistamo; Otaniemi 1994

Helsinki University of Technology
Department of Computer Science
Digital Systems Laboratory
Otaniemi, Otakaari 1
SF–02150 ESPOO, FINLAND

Phone: $\frac{90}{+358\text{–}0}$ 4511
Telex: 125 161 htkk sf
Telefax: +358–0–465 077
E-mail: lab@hutds.hut.fi

Preface

The work covered in this thesis has been carried out at the Digital Systems Laboratory of Helsinki University of Technology during 1990–1993. I am grateful to the head of the laboratory, Prof. Leo Ojala, for providing excellent working conditions and for supporting me during this period. My thanks also go to all colleagues—former and present—for the inspiring and intellectual atmosphere in our laboratory; I especially wish to thank Dr. Nisse Husberg for his supervising help when I wanted to take part in the research activities of the laboratory back in 1989.

I must express special gratitude to Dr. Iiro Honkala for his help in my work. I have been very fortune to get his valuable comments on many of my preliminary results; a thick folder consisting of his letters will always remind me of our numerous fruitful discussions. I very much appreciate the discussions with Heikki Hämäläinen and Markku Kaikkonen on football pool systems and other coding theory issues. It was a true pleasure to co-author one of the papers in this thesis with Heikki. I thank Elizabeth Heap-Talvela for checking the English language of the thesis.

I also thank the Foundation of Technology, the Engineering Society in Finland TFiF, the Oscar Öflund Foundation, the Ella and Georg Ehrnrooth Foundation, the Helsingin Sanomat Centenary Foundation, and the Academy of Finland for their financial support during this work.

Finally, I am very grateful to my family and my friends, who have all supported me throughout this work.

Espoo, August 1993

Patric Östergård

Contents

List of Publications

This thesis consists of a summary and the following publications:

[P1] P. R. J. Östergård, A new binary code of length 10 and covering radius 1, *IEEE Transactions on Information Theory* **37** (1991), 179–180.

[P2] P. R. J. Östergård, Upper bounds for q-ary covering codes, *IEEE Transactions on Information Theory* **37** (1991), 660-664; and **37** (1991), 1738.

[P3] P. R. J. Östergård, Further results on (k, t)-subnormal covering codes, *IEEE Transactions on Information Theory* **38** (1992), 206–210.

[P4] P. R. J. Östergård, Construction methods for mixed covering codes, in M. Gyllenberg and L. E. Persson (eds.), "Proceedings of the 21st Nordic Congress of Mathematicians," Marcel Dekker, New York, 1993, to appear.

[P5] P. R. J. Östergård, New upper bounds for the football pool problem for 11 and 12 matches, *Journal of Combinatorial Theory. Series A*, to appear.

[P6] P. R. J. Östergård and H. O. Hämäläinen, New upper bounds for binary/ternary mixed covering codes, Research Report A 22, Digital Systems Laboratory, Helsinki University of Technology, 1993.

Papers [P1] to [P5] were written without co-authors. The mathematical theory in [P6] was developed by the author of the thesis, who also wrote the paper. The ideas behind the constructions and the new codes in the same paper are due to both authors.

1 Introduction

In 1948, Taussky and Todd [86] considered the following group-theoretic problem: Let G be an Abelian group with n independent generators $g_1, g_2, \ldots, g_n$, each of order q. A subset H of G is said to cover G if, for every $g \in G$, there is an $h \in H$ such that $g = hg_i^\alpha$ for some $1 \leq i \leq n$, $0 \leq \alpha \leq q-1$. The problem is now, for given n and q, to find the minimum cardinality of a covering set H: $\sigma(n,q)$. If it is further required that H be a subgroup of G, the minimum cardinality is denoted by $\sigma^*(n,q)$. In this group-theoretic context, the problem has been discussed in a variety of papers, for example, [17, 67, 69, 70, 80, 98, 99].

Actually, long before the paper [86] by Taussky and Todd appeared there was a big interest in this problem among football pool enthusiasts in the Nordic countries. In the football pool game you have to guess the outcome of—usually 12 or 13—football matches. For each match there are three alternatives: you mark a '1' if you think that the home team will win, an 'x' if you think that the teams will draw, or a '2' if you think that the away team will win. If your guess is correct, you win the first prize; if the outcome of exactly one match differs from your guess, you win the second prize, etc. Usually, there are 3 or 4 prize classes. Now the following combinatorial question follows very naturally: If there are n matches on a football pool coupon, what is the minimum number of guesses (by a guess is still meant an estimate of the outcome of all matches) such that, for any outcome of the matches, you will win at least the jth prize? A collection of guesses is usually called a *football pool system*. For further discussion of the early history of such systems, see [27, 94].

The aforementioned problem of constructing football pool systems is more general than the original problem proposed by Taussky and Todd. Namely, a set $H \subseteq G$ must be found which has the property that, for every $g \in G$, there is an $h \in H$ such that $g = hg_{a_1}^{\alpha_1} g_{a_2}^{\alpha_2} \cdots g_{a_{j-1}}^{\alpha_{j-1}}$ for some $1 \leq a_1 < a_2 \cdots < a_{j-1} \leq n$, $0 \leq \alpha_i \leq q-1$. A football pool system is now obtained from a covering set H by encoding all elements according to, for example, the following scheme: $g_i^0 \rightarrow$ '1', $g_i^1 \rightarrow$ 'x', and $g_i^2 \rightarrow$ '2'. As a matter of fact, the source of inspiration for research in this area was from the very beginning the problem of constructing football pool systems. Taussky and Todd [86] refer to this problem as a "certain industrial problem," however, in a paper by Mattioli [69], published in 1950, the connection is explicitly stated.

Given a set G and the covering properties that have to be fulfilled, the problem of finding the minimum cardinality of a covering set H is far from trivial. Exact values have been obtained only in some special cases, mostly for small values of the parameters. In the general case, efforts have been concentrated on obtaining good upper and lower bounds on the minimum cardinality. Good lower bounds can be obtained by a variety of analytic methods [12, 15, 16, 32, 34, 42, 43, 58, 90, 92, 96, 100, 102]; upper bounds, on the other hand, are found by explicitly constructing a covering set. In this work, new construction methods are developed, thereby improving many upper bounds.

A survey of construction methods for covering codes was given by Cohen *et al.* in [16]; some later results were surveyed by Van Lint in [62]. In this thesis, these surveys are not only brought up-to-date by including the results in [P1] to [P6] and others' new results, but new light is also shed on some old methods.

In Section 2 an exact mathematical formulation (in a combinatorial context) of the problem is given. The construction methods are presented in Sections 3 to 6. These are divided into the following groups: computer search for covering codes is discussed in Section 3, partitioning constructions are given in Section 4, a matrix method is presented in Section 5, and, finally, some other combinatorial methods are listed in Section 6. The thesis is concluded in Section 7.

2 Covering Codes

In the earliest papers, the covering problem presented in the Introduction was discussed using the aforementioned group-theoretic notations. However, as pointed out, the problem can also be considered from a purely combinatorial point-of-view. In the 1960's, discussions of the covering problem in a combinatorial context became more and more common ([87], etc.); with the years, this has become the predominant approach. Consequently, this approach and its established notations are used throughout this thesis. There should, however, be no problem in seeing the one-to-one correspondence between the two approaches.

In this section, codes over spaces where all coordinates are of the same arity are first considered. Subsequently, codes over mixed alphabets, *mixed covering codes*, are discussed. For a thorough introduction to coding theory, see [61, 68, 74].

2.1 Nonmixed Covering Codes

Let F_q^n be an n-dimensional space over F_q, an alphabet consisting of q elements. If q is a prime power, F_q is the finite field of q elements (also called the

Galois field of q elements: GF(q)), otherwise F_q is the set of integers modulo q. In any case, the set $F_q = \{0, 1, \ldots, q-1\}$ is used to denote the elements of the alphabet. A *word* in this space is an n-tuple $x = (x_1, x_2, \ldots, x_n)$, where $x_i \in F_q$; such a word is often written in a shorter form $x_1 x_2 \cdots x_n$. A *code* C is now a nonempty subset of F_q^n: $\phi \neq C \subseteq F_q^n$. The elements in C are *codewords*, and the *length* of the code is n. Actually, in some cases it is necessary to define codes as multisets, that is, to allow multiple occurrences of codewords in the code, however, in this thesis such codes are not considered.

The *Hamming distance* $d(x, y)$ between two words $x, y \in F_q^n$ is the number of coordinates in which they differ. The *weight* of a word $x \in F_q^n$ is $wt(x) = d(x, 0)$, that is, the number of nonzero coordinates ($0 = (0, 0, \ldots, 0)$). The Hamming distance function is a *metric*, since for all $x, y, z \in F_q^n$,

1. $d(x, y) \geq 0$,
2. $d(x, y) = 0$ iff $x = y$,
3. $d(x, y) = d(y, x)$, and
4. $d(x, z) \leq d(x, y) + d(y, z)$.

A code $C \subseteq F_q^n$ is said to cover F_q^n with *covering radius* R if every word in F_q^n is within Hamming distance R from some codeword in C, and if this is not fulfilled for $R' = R-1$. Such a code is called a $(q, n, M)R$ code, where $M = |C|$ is the *cardinality* of the code. If all words in F_q^n have at least μ codewords within Hamming distance R, the code is said to be a μ-fold multiple covering. Multiple coverings are discussed, for example, in [14, 25, 26, 95]. Furthermore, the notation

$$K_q(n, R) = \min\{M \mid \text{there is a } (q, n, M)R \text{ code}\}$$

is used. The index q is usually omitted in the binary case. Other notations that have been used in the literature include $\sigma(n, k) = K_k(n, 1)$, $\sigma_n = K_3(n, 1)$ (for example, in [56, 97]; see also the Introduction), and $\gamma(n, k, s) = K_k(n, n-s)$ [9, 10]. The determination of $K_3(n, 1)$ is usually referred to as the *football pool problem*; see [21, 49, 50, 56, 89, 97] and [P5, P6]. A $(q, n, M)R$ code with $M = K_q(n, R)$ codewords is called *optimal*.

In the earliest papers only codes with covering radius 1 were treated. In the early 1970's, the following exact values of $K_q(n, 1)$ were known: $K_q(2, 1) = q$ and $K_q(3, 1) = \lceil (q^2 + 1)/2 \rceil$ [46]; $K_q((q^k - 1)/(q - 1), 1) = q^{(q^k-1)/(q-1)-k}$, if q is a prime power and $k \geq 2$ [69, 70, 98, 99], see also [67] (the Hamming codes); $K_{pq}(q+1,1) = p^q q^{q-1}$, if q is a prime power [48, 76], see also [4]; $K_2(4,1) = 4$ and $K_2(5,1) = 7$ [86]; $K_2(6,1) = 12$ [83]; $K_2(8,1) = 32$ [84]; $K_3(5,1) = 27$ [49]; and $K_4(4,1) = 24$ [82]. The fact that the only result that has been added to this list during the last two decades is $K_2(2^k,1) = 2^{2^k-k}$ [90] clearly indicates the complexity of calculating exact values of $K_q(n,R)$.

Having determined the value of $K_q(n,R)$ for given parameters, it is also interesting to know the number of nonequivalent optimal covering codes with these parameters. Two codes, C and C', are equivalent if C' can be obtained from C by a permutation of the coordinate positions and a permutation of the elements of F_q in each coordinate position. Stanton and Kalbfleisch [83] enumerated all binary optimal covering codes up to equivalence for $R = 1$ and $n \leq 5$; the fact that there is a unique $(2,7,16)1$ covering code—the binary Hamming code of length 7—was proved in an early paper by Zaremba [99]. Kalbfleisch and Stanton [46] proved that the ternary Hamming code of length 4 is a unique $(3,4,9)1$ covering code. Recently, Kolev [54] constructed all nonequivalent $(3,5,27)1$ covering codes. Finally, it is known [73] that the number of nonequivalent $(2, n = 2^k-1, 2^{2^k-k-1})1$ codes is at least $2^{2^{cn}}$, for some constant $0 < c < 1$.

By considering the total number of words in a space and the number of words covered by a codeword in the space, the following well-known *sphere covering bound* is obtained.

Theorem 1 $K_q(n,R) \geq q^n / \sum_{i=0}^{R} (q-1)^i \binom{n}{i}$.

The number of codewords in a code divided by the bound in Theorem 1 is called the *density* (μ) of the code. Apparently, $\mu \geq 1$. If q is a prime power, then the density of an optimal code with covering radius 1 approaches 1 as n goes to infinity [45]; see also [71]. A covering code with density $\mu = 1$ is called *perfect*. For any word in the space, exactly one codeword of a perfect code is within Hamming distance R from this word. In the early 1970's, Tietäväinen and Van Lint showed that if q is a prime power, then the only nontrivial perfect codes are codes with the same parameters as the Hamming and Golay codes; see [60] for a survey of these results.

In the binary case an n-dimensional space can be displayed as a hypercube of dimension n (an *n-cube*). There is now a one-to-one mapping between the nodes in the n-cube and the words in the space, so that two nodes are adjacent exactly when the corresponding codewords differ in one coordinate (are at Hamming distance 1 from each other). In Figure 1 this is illustrated for $n = 4$. The black nodes of the graphs indicate the codewords of a $(2,4,4)1$ code. Thus $K(4,1) = 4$, since by Theorem 1, $K(4,1) \geq 16/5$.

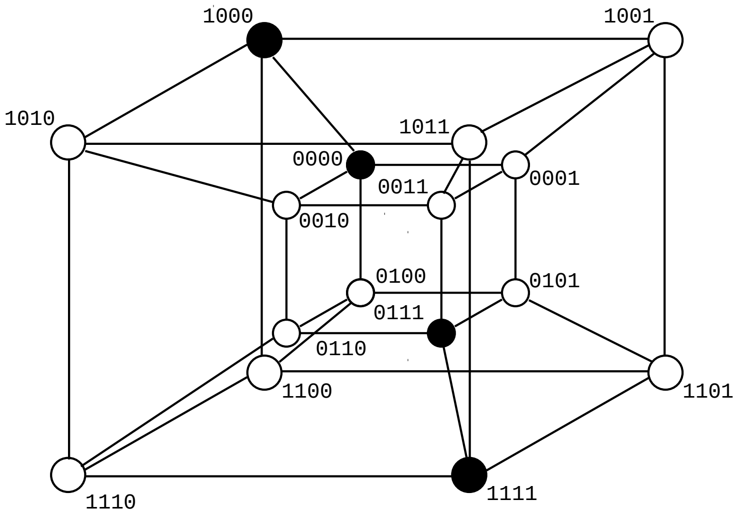

Figure 1: Hypercube of dimension 4.

If a code is a linear subset of the space, it is called a *linear code*. A linear code that has q^k (q is a prime power) codewords and covers F_q^n with covering radius R is called an $[n,k]R$ code. In this thesis it is not required that the codes be linear. Upper and lower bounds on binary linear covering codes have been considered in [6, 7, 8, 15, 24, 101].

2.2 Mixed Covering Codes

Consider a space $H = F_{q_1}^{n_1} F_{q_2}^{n_2} \cdots F_{q_m}^{n_m}$, with $m \geq 1$, $n_i \geq 0$, $\sum_{i=1}^{m} n_i \geq 1$, and $q_i \geq 2$. If $m \geq 2$ and there are indices $i, j \leq m$ such that $q_i \neq q_j$, the space is a *proper* mixed space. Similarly to the nonmixed case, a mixed code $C \subseteq H$ is said to cover H with *covering radius* R if every word in H is within Hamming distance R from some codeword in C, and if this is not fulfilled for $R' = R-1$; such a code is called a $(q_1, q_2, \ldots, q_m; n_1, n_2, \ldots, n_m; M)R$ code. Furthermore, $K_{q_1,q_2,\ldots,q_m}(n_1, n_2, \ldots, n_m; R) = \min\{M \mid$ there is a $(q_1, q_2, \ldots, q_m; n_1, n_2, \ldots, n_m; M)R$ code$\}$. Results for nonmixed codes can in many cases directly be generalized to the mixed case; for example, the sphere covering bound is as follows.

Theorem 2 $K_{q_1,q_2,\ldots,q_n}(1, 1, \ldots, 1; R) \geq (\prod_{i=1}^{n} q_i)/V(R)$,
where $V(R) = 1 + \sum_{j=1}^{R} \sum_{1 \leq i_1 < i_2 < \cdots < i_j \leq n} (q_{i_1} - 1) \cdots (q_{i_j} - 1)$.

A lot of research has been done on mixed covering codes, however, for a long period of time research only considered perfect mixed codes. Perfect mixed codes have been discussed, for example, in [20, 28, 29, 30, 31, 57, 59, 85, 93]. During the last decade, there has been an increasing interest in mixed covering codes, especially in binary/ternary codes [27, 64, 92]. Binary/ternary covering codes are useful as football pool systems if one of the three possible outcomes for some matches is excluded by the gambler. For this case, the notation $K(t, b, R) = K_{3,2}(n_1, n_2; R)$ is used in [27, 64].

The construction methods to be presented in Sections 3 to 6 are mainly given for nonmixed covering codes. This is done to keep the presentation plain. In cases where the generalization of a method to the mixed case is not clear or is not even possible, this is mentioned after the presentation of the method. Some constructions that are only applicable to mixed covering codes are also given. Thorough considerations of construction methods for general mixed covering codes and binary/ternary mixed covering codes can be found in [P4] and [P6], respectively.

Finally, the mixed codes are not only interesting in their own right, but many times good (best known) nonmixed covering codes can be constructed out of mixed covering codes, see [20] and [P1,P4,P6] (one useful theorem is given in Section 4.2).

3 Computer Search for Covering Codes

The problem of finding a $(q, n, M)R$ code (with q, n, M, and R fixed) can be seen as a combinatorial optimization problem. Such problems have a finite set of feasible solutions and a cost function that attaches a cost to each such solution. It is now very natural to let the feasible solutions be the set of M-element subsets of F_q^n and, for a solution C in this set, to set the cost function to be the number of uncovered words in the space:

$$\mathrm{cost}(C) = \{x \in F_q^n \mid d(x, C) > R\}.$$

If there is a code C such that $\mathrm{cost}(C) = 0$, then C is a covering code with the given parameters. Now, any method for combinatorial optimization can be used to find a covering code (see, for example, [72]).

To find out not only an upper bound on $K_q(n, R)$, but the exact value of the function, an M must be found such that there is a $(q, n, M)R$ code but there is no $(q, n, M-1)R$ code. Whereas the proof of existence is constructive, other (mainly analytic) methods have to be used in the nonexistence proof. Different methods, like linear programming [16, 100, 102], have been used in such proofs. In most cases, the best that can be done is to prove the nonexistence of a $(q, n, M-a)R$ code, where $a > 1$ so that there is a gap between the best known upper and lower bounds.

An approach that is used in [P6] to settle some values of $K_{3,2}(n_1, n_2; R)$ is now presented, followed by an approach which can be used only to give upper bounds.

3.1 A Set Covering Approach

The problem of finding minimal covering codes can be seen as a special case of the *set covering problem* (SCP) [2, 3, 13, 19]. In the SCP an $m \times n$ zero-one matrix a_{ij} and a cost function c_j associated with the columns are given; the problem is now to cover the rows by a subset of columns at minimum cost.

In the search for a minimal $(q, n, M)R$ code a $q^n \times q^n$ matrix is constructed, where the columns and the rows are labeled with the words in F_q^n (in lexicographic order, for example). The entry a_{ij} is 1 if the Hamming distance between the labels of the ith row and the jth column is less than or equal to R, 0 otherwise. The cost function is $c_j = 1$: it is a *unicost problem.* To find out the value of $K_2(4, 1)$ (which was already shown to be 4), the matrix in Figure 2 is constructed.

Unfortunately, the facts that this is a unicost problem, that all rows and columns have the same number of ones, and that the instances are in many senses symmetrical, together collaborate to make the problem of finding a minimal covering very hard. Although many SCP instances can be solved reasonably fast, this is generally not the case for covering codes. However, for small covering codes this approach can be used as shown in [P6], where some exact bounds are proved by computer search. The heuristics of the search is based on ideas from [81], where a search for covering designs was carried out.

In cases where the exact value of $K_q(n, R)$ cannot in reasonable time be found by methods that solve the SCP, efforts can be made to improve upper bounds on this function by implicitly constructing good covering codes. In the search for such codes, *probabilistic methods* have turned out to perform very well.

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
0000	1	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0
0001	1	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0
0010	1	0	1	1	0	0	1	0	0	0	1	0	0	0	0	0
0011	0	1	1	1	0	0	0	1	0	0	0	1	0	0	0	0
0100	1	0	0	0	1	1	1	0	0	0	0	0	1	0	0	0
0101	0	1	0	0	1	1	0	1	0	0	0	0	0	1	0	0
0110	0	0	1	0	1	0	1	1	0	0	0	0	0	0	1	0
0111	0	0	0	1	0	1	1	1	0	0	0	0	0	0	0	1
1000	1	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0
1001	0	1	0	0	0	0	0	0	1	1	0	1	0	1	0	0
1010	0	0	1	0	0	0	0	0	1	0	1	1	0	0	1	0
1011	0	0	0	1	0	0	0	0	0	1	1	1	0	0	0	1
1100	0	0	0	0	1	0	0	0	1	0	0	0	1	1	1	0
1101	0	0	0	0	0	1	0	0	0	1	0	0	1	1	0	1
1110	0	0	0	0	0	0	1	0	0	0	1	0	1	0	1	1
1111	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1

Figure 2: Covering matrix for $K_2(4,1)$.

3.2 A Probabilistic Approach

In the early 1980's, Černy [11] and Kirkpatrick [53] independently presented a probabilistic method for combinatorial optimization problems: *simulated annealing* (SA) [1, 55]. The first results on the use of SA in the search for codes are due to El Gamal *et al.* [18]. They considered source codes, constant weight codes, and spherical codes.

In 1987, Wille [97] used SA to find a $(3,6,74)1$ code, thus proving that $K_3(6,1) \leq 74$. This was a good improvement on $K_3(6,1) \leq 79$, which was the best known upper bound at that time (actually, among football pool constructors in the Nordic countries it was known that $K_3(6,1) \leq 75$, which had been proved by S. Solbrand). These results encouraged further research on the construction of covering codes by SA; the aforementioned upper bound was later improved to 73 independently by Van Laarhoven *et al.* [56] and the author of this thesis (see [27, Table I]).

SA has turned out to be an important tool in the search for covering codes; see [P4] for a more detailed treatment of the use of SA in the search for covering codes. The $(4,2;1,7;60)1$ code given in [P1] was found by SA. Simulated annealing has been used to construct a large number of codes in the papers

[P2,P4,P6]. SA further plays an important role in some of the methods to be presented in the sequel. Also, as pointed out in [P6], combinatorial constructions can sometimes be used to obtain a code that leaves only a small number of words uncovered; SA can then be used to find a good covering of these words.

As a consequence of the probabilistic nature of SA, codes found in repeated searches are not necessarily equivalent. The method can thus be used to find nonequivalent covering codes with given parameters, whenever such exist.

4 Partitioning Constructions

In partitioning constructions old codes are partitioned into subcodes and combined. These constructions work efficiently whenever certain conditions for the partitions are fulfilled. Such constructions are very useful among many types of codes, for example, error-correcting codes [79] and constant weight codes [5, 75]; it is thus very natural to search for analog methods for covering codes.

The classification of codes according to properties of their partitions is first shown. Thereafter, constructions using these codes are briefly discussed. For mixed covering codes, the definitions and constructions are essentially similar.

4.1 Normal, Seminormal, and Subnormal Codes

A partitioning construction for binary *linear* codes was first presented by Graham and Sloane in [24]: the *amalgamated direct sum* (ADS) construction efficiently combines so called *normal* codes. These concepts were later generalized to the nonlinear case in [16]. In the ADS construction, the codes are partitioned according to the values of given coordinates. In [32] Honkala introduces *subnormal* binary codes, and shows that normal binary codes consist of a subset of subnormal binary codes.

Definition 1 *A* $(2, n, M)R$ *code* C *is subnormal if there are nonempty subcodes* C_1 *and* C_2*, such that* $C = C_1 \cup C_2$ *and for all* $x \in F_2^n$*,* $d(x, C_1) + d(x, C_2) \leq 2R + 1$.

Actually, in the original definition the subcodes are allowed to be empty [32, 34], however, since the constructions in which subnormal codes are involved generally require the subcodes to be nonempty, this requirement is included in the definition. In [66] Lobstein and Van Wee generalize the concepts of normal codes and subnormal codes (Definition 1) to q-ary codes.

Definition 2 *A $(q, n, M)R$ code C is subnormal if there are nonempty subcodes $C_1, C_2, \ldots, C_q$, such that $C = C_1 \cup C_2 \cup \cdots \cup C_q$ and for all $x \in F_q^n$, $\sum_{i=1}^{n} d(x, C_i) \leq qR + q - 1$.*

The comment on nonemptiness after Definition 1 also holds for this definition. The ADS construction is easily generalized to the q-ary case as shown in [66]. Unfortunately, it turns out that, for example, no nonbinary nontrivial perfect codes are subnormal, so it seems that partitioning constructions cannot be used in the q-ary case to the same extent as in the binary case. The following idea, however, opens the door to some new results, which show that partitioning constructions are of use also in this case. The last expression of Definition 1 can be written as $\min_i d(x, C_i) + \max_i d(x, C_i) \leq 2R + 1$, leading to another generalization of the same definition.

Definition 3 *A $(q, n, M)R$ code C is subnormal if there are nonempty subcodes $C_1, C_2, \ldots, C_q$, such that $C = C_1 \cup C_2 \cup \cdots \cup C_q$ and for all $x \in F_q^n$, $\min_i d(x, C_i) + \max_i d(x, C_i) \leq 2R + 1$.*

The first steps towards a generalization in this direction were taken in [P2, Definition 1]; that definition equals Definition 3, except that $d(x, C) = R$ was used instead of $x \in F_q^n$. Such codes are named *seminormal*; subnormal codes are apparently seminormal, but not necessarily vice versa.

Not only was a partition of C into q subcodes considered in [P2]; more generally, the notation of *k-seminormality* was used for codes partioned into k (arbitrary) rather than q subcodes, The following very general definition is from [35], with the additional parameter R' introduced in [P3]. (In [P3, Section III], an even more sophisticated generalization, (k, t, R'')-subnorm, is given, however, the parameter R'' is hardly ever significant, so it is omitted here.)

Definition 4 *A $(q, n, M)R$ code C has (k, t)-subnorm (S, R') if there is a partition of C into k nonempty subsets $C_1, C_2, \ldots, C_k$ such that $\min_a d(x, C_a) + \max_a d(x, C_a) \leq S$ whenever $R - t \leq d(x, C) \leq R$, and, for all x, $\max_a d(x, C_a) \leq R'$.*

Such a partition is called *acceptable*. A code C is said to be (k, t)-subnormal if it has (k, t)-subnorm $(2R+1, R')$ (for some R'; the parameter R' is then usually omitted). Thus, $(k, 0)$-subnormality coincides with k-seminormality. Furthermore, a code is called *strongly seminormal* [P2,P3] if it has (k, R)-subnorm $(2R + 1, R + 1)$. An interesting question is whether the parameter t in Definition 4 is significant. It seems that there are very few—especially optimal—codes, that have (k, a)-subnorm S, but that do not have (k, b)-subnorm S,

$a \neq b$. A necessary condition for this to be true is that $a < b$. Altogether, such codes exist. The $(3,6,3)4$ repetition code $\{000000, 111111, 222222\}$ has (3,0)-subnorm 8, but has (3,1)-subnorm S only for $S \geq 9$. An algorithm using simulated annealing for finding partitions of k-seminormal codes is given in [P3, Section IV].

The concept of normality was mentioned very briefly earlier. Although generally not as important as subnormality in the construction of nonlinear covering codes, normality plays an important role in some efficient constructions, for example, in [P3, Corollary 3]. The definition of (k,t)-norm is here stated as in [P3, Definition 2].

Let C be a $(q,n,M)R$ code with $C_a^{(i)\prime} = \{(c_1,\ldots,c_{i-1},c_{i+1},\ldots,c_n) \mid (c_1,\ldots,c_{i-1},a,c_{i+1},\ldots,c_n) \in C\}, a \in F_q$. These sets are assumed to be nonempty for all a.

Definition 5 *The code C has (q,t)-norm $(N^{(i)}, R_i')$ with respect to the i^{th} coordinate if* $\min_a d(x, C_a^{(i)\prime}) + \max_a d(x, C_a^{(i)\prime}) \leq N^{(i)}$ *whenever* $R - t \leq d(x, \bigcup_a C_a^{(i)\prime}) \leq R$, *and, for all x,* $\max_a d(x, C_a^{(i)\prime}) \leq R_i'$. *If $N^{(i)} \leq N, R_i' \leq R'$ for at least one coordinate i, C is said to have (q,t)-*norm (N, R'), *and coordinates for which this equation holds are called* acceptable.

A code C is said to be (q,t)-normal if it has (q,t)-norm $2R$ (the value of R' is here not essential). As can be seen, the first parameter (k) in the definition of (k,t)-norm is superfluous in the nonmixed case as it is always q, however, in the mixed case its presence is justified.

A lot of research has been done—mainly on binary covering codes—to determine normality and subnormality properties of (optimal and other) covering codes [24, 33, 35, 36, 38, 40, 41, 44, 51, 52, 66, 78, 91]. Also, as pointed out in [P6], some early results by Golomb and Posner [23] actually deal with partitions of covering codes.

4.2 Combining Codes

Codes with the aforementioned properties—normality, seminormality, and subnormality—can now efficiently be combined to obtain record-breaking codes. The constructions act on codes, say A and B, that are partitioned into blocks of codewords: $A = A_1 \cup A_2 \cup \cdots \cup A_k$ and $B = B_1 \cup B_2 \cup \cdots \cup B_k$. For all i, all words in A_i and B_i are combined to get $C = \cup_{i=1}^{k} (A_i \oplus B_i)$. Now, if the aforementioned partitions are acceptable partitions corresponding to (k,t)-(sub)norms (N_A, R_A') and (N_B, R_B'), an upper bound on the covering radius of C can be calculated by combinatorial arguments. It turns out that especially (q, R)-normal [P3, Corollary 3], seminormal [P2, Theorem 3], strongly seminormal [P2, Theorem 4], and (q, R)-subnormal [P3, Theorem 1] covering codes are important building blocks. In [35] Honkala names this construction *blockwise direct sum* (BDS). The ADS construction mentioned earlier is a BDS construction where at least one of the codes involved is partitioned according to the values of one of its coordinates (cf. (k, t)-norm).

By using cosets of a Hamming code as one of the codes that are combined, the following very useful theorem can be obtained [P4, Theorem 17].

Theorem 3 *If q is a prime power and $k \geq 2$, then* $K_{q_1=q,q_2=q^k,\ldots,q_m}(n_1 + (q^k-1)/(q-1), n_2, \ldots, n_m; R) \leq q^{(q^k-1)/(q-1)-k} \cdot K_{q_1=q,q_2=q^k,\ldots,q_m}(n_1, n_2 + 1, \ldots, n_m; R)$.

The theorems in [P1] are special instances of this theorem. Similar constructions are also discussed in [20]. The partitioning constructions and the definitions of different degrees of normality given here can without difficulties be carried over to the mixed case; details can be found in [P4].

5 A Matrix Method

The possibility of using computers in the search for covering codes was discussed in Section 3. Simulated annealing works very well as long as the codes are relatively small (for example, up to about 100 codewords for $R = 1$) but the performance deteriorates quite fast with an increasing number of codewords. One solution to this problem is to search for a code with some kind of structure imposed on it. A search could be carried out for, for example, a *self-complementary* code. A binary code is self-complementary if $c + 11\cdots1$ is a codeword whenever c is a codeword. The code in Figure 1 has this property. The requirement can be rewritten in the following way: $c + 11\cdots1$ is a codeword whenever $c + 00\cdots0$ is a codeword, so the code consists of cosets of the linear code $\{00\cdots0, 11\cdots1\}$. By using the matrix method, codes that consist of cosets of a linear code can be found.

The first ideas that led to this method were presented by Kamps and Van Lint [50] in 1969; these ideas were later refined by Blokhuis and Lam [4] in 1984. Blokhuis and Lam considered the construction of q-ary codes with covering radius 1. The method is easily generalized to many cases as shown in [10, 63] (arbitrary covering radius), [25, 26] (different kinds of multiple coverings), and [P4,P6] (mixed codes). For arbitrary covering radius the following holds:

Let $A = (I; M) = (a_1, \ldots, a_n)$ be a $r \times n$ matrix where I is the $r \times r$ identity matrix and M is an $r \times (n - r)$ matrix with entries from F_q. Now, for $s \in F_q^r$,

$$S_{A,R}(s) = \{s + \sum_{j=1}^{n} \alpha_j a_j \mid \alpha_j \in F_q, |\{j \mid \alpha_j \neq 0\}| \leq R\},$$

and s is said to *R-cover $S_{A,R}(s)$ using A*. Consequently, $A = I$ corresponds to covering in the traditional sense. A subset S of F_q^r is said to *R-cover F_q^r using A* if

$$F_q^r = \bigcup_{s \in S} S_{A,R}(s).$$

Theorem 4 (Carnielli [10, Theorem 2.1], Van Lint Jr. [63, Theorem 1.4.4]) *If S R-covers F_q^r using an $r \times n$ matrix $A = (I; M)$, then $W = \{w \in F_q^n \mid Aw \in S\}$ covers F_q^n with radius R. $|W| = |S| \cdot q^{n-r}$.*

It is far from obvious how to make use of this theorem in practice. First, when attempts are made to improve a certain bound $K_q(n, R) \leq M$, the value of r must be fixed. After that, both the elements of the set S and a matrix M that lead to a covering have to be found.

In [4] the method is used to prove that $K_3(7, 1) \leq 216$. The heuristics is not explained; the authors only mention that the code was found in a computer search. In [56] simulated annealing is used; during the search both the words in S and the columns of A are altered. By using this approach a record-breaking $(3, 8, 486)1$ code was found.

In [P5] the fact that the method gives us a code that consists of cosets of a linear code is utilized. Then all nonequivalent linear codes [22, 77] with given parameters can be considered, and a search can be carried out by simulated annealing with the matrix A fixed to parity check matrices for these codes, one at a time. Unfortunately, the problem of finding all such nonequivalent codes is a very hard problem. The following restriction is then made: only linear codes with different weight distributions are considered. This *invariant* is quite *sensitive*—all nonequivalent codes cannot be distinguished but most of them—and the codes can be found quite efficiently. The results also encourage the approach: two new upper bounds for the football pool problem were found in [P5] and many new binary/ternary covering codes were found in [P6]. It is further interesting to see that the linear code used in the proof of $K_3(11, 1) \leq 9477$ in [P5] has the same length and the same number of codewords as the $(3, 11, 729)2$ Golay code, however, these are not equivalent.

Thus, cosets of good linear codes (small covering radius) do not necessarily lead to the most efficient coverings.

The $(5,5,35)2$ code given in [P2] was actually found by this method. It consists of a union of 7 cosets of a linear code. If (a,b,c,d,e) is a codeword in the code, so is $(a+1,b+1,c+1,d+1,e)$ (mod 5). The bound $K_3(7,1) \leq 186$, which was proved in [56], can also be proved by the matrix method. With $|S| = 62$, $r = 6$ and $n = 7$, coverings can be found with $M = (111000)^T$ and $M = (111110)^T$. Actually, the second code in [56, Fig. 2] consists of 62 cosets of a linear code. In the search for $(3,7,186)1$ codes in [56], approximately 100 h of CPU time on a VAX 11/785 computer was used to find two codes. By the matrix method, codes are found considerably faster.

In the mixed case, as explained in [P4,P6], care must be taken when choosing the matrices. Arities are associated with the rows and the columns of A, and an entry of A can have a nonzero value of F_q only if the arities associated with the row and the column of the entry both are q.

6 Other Combinatorial Methods

A wide variety of combinatorial construction methods has been published through the years. In this section, methods that can be generally applied and bounds obtained by such methods are presented.

6.1 Some Direct Constructions

General upper bounds corresponding to constructions of good q-ary covering codes with $n - R$ large are first presented. Theorem 5 is trivial; Theorems 6 and 7 are given in [12, Theorem 6] and [P2, Theorem 6], respectively.

Theorem 5 $K_q(n,R) = 1$, *if* $n \leq R$.

Theorem 6 $K_q(n,R) = q$, *if* $R+1 \leq n \leq R + \lceil n/q \rceil$.

Theorem 7 $K_q(qr-p, qr-r-p-1) \leq q(p+2)$, *if* $0 \leq p \leq q-2$.

See [P4] for corresponding bounds for mixed codes. Some upper bounds that correspond to constructions that can be applied directly to existing covering codes are now given. Theorem 10 cannot be generalized to the mixed case, whereas Theorem 11 explicitly concerns mixed codes.

Theorem 8 $K_q(n, R+1) \leq qK_q(n, R)$.

Theorem 9 $K_q(n_1 + n_2, R_1 + R_2) \leq K_q(n_1, R_1)K_q(n_2, R_2)$.

Theorem 10 $K_{qs}(n, R) \leq s^{n-1}K_q(n, R)$.

Theorem 11 $K_{q_1,q_2,\ldots,q_m}(n_1, n_2 + 1, \ldots, n_m; R) \leq (q_2/q_1)K_{q_1+1,q_2,\ldots,q_m}(n_1, n_2, \ldots, n_m; R)$, *if* $q_2 > q_1$.

Theorems 8 and 9 are trivial; Theorem 9 is obtained by combining codes using the *direct sum construction* [68, p. 76], and Theorem 8 can be obtained as a special case of Theorem 9 (see [P4, Theorem 10]). Theorem 8 is mentioned in the seminal paper of Taussky and Todd [86] (for $R = 1$). Theorem 10 is proved in [4] (for $R = 1$). Theorem 11 and a slight modification of it are discussed in [P4,P6].

A good upper bound is obtained by Theorem 10 in cases where the bound $K_q(n, R)$ is good; starting from a q-ary Hamming code of length $q + 1$, inequality can be replaced by equality in Theorem 10. By a construction similar to that in the proof of Theorem 10 ([82, Theorem 1]), one can—starting from the aforementioned Hamming codes—not only get good codes of arity qs, but of any arity greater than q [47, 82].

6.2 Piecewise Constant Codes

The concept of piecewise constant codes was introduced in [16]. The coordinates of such a code are partitioned into t blocks. Now, if c is a codeword, then all words that can be obtained by all possible permutations among the coordinates of one block are also codewords. The following code is an example of a $(2, 5, 7)1$ piecewise constant code (with $t = 2$):

00 011	01 000	11 000	11 111
00 101	10 000		
00 110			

In [16] a useful graphical method for determining the covering radius of a piecewise constant code is presented. The fact that permutations of coordinates leave the code unchanged means that the code has a nontrivial automorphism group. An automorphism group of the aforementioned $(2, 5, 7)1$ code can be generated by the permutations $(1, 2)$, $(3, 4)$, and $(3, 5)$; the order of the group is 12. The code is obtained by applying these permutations to, for example, the following set of words: $\{00000, 00111, 10000, 11011\}$. It is interesting to see that the code can be generated by applying the group generated by $(1,2)(3,4,5)$ to these words; the order of this group is only 6.

The other codes in [16] that are given as constant weight codes can also be described nicely by a single generator. The $(2,6,12)1$ code in [16, Fig. 3] is obtained by applying the group generated by $(1,2,3)(4,5,6)$ to $\{000100, 100111, 011000, 111011\}$. The $(2,11,192)1$ code in [16, Fig. 7] can be constructed so that $(2,3,4,5,6)(7,8,9,10,11)$ is an automorphism group. The crucial part is that there is a Steiner system $S(4,5,11)$ with the aforementioned automorphism group [88].

Apparently no exhaustive study of the use of automorphism groups in the search for good covering codes has been performed. The examples presented here encourage research in this area; this method could possibly be a good alternative to the matrix method in the search for large codes.

6.3 Lengthening Constructions

It is easily shown that if C is a $(q,n,M)R$ code (q is a prime power), then $C \oplus \{0\}$ R-covers F_q^{n+1} using the $(n+1) \times (qn+1)$ matrix

$$A = \begin{bmatrix}
1 & & & 1 & & & 2 & & & & q-1 & & & 0 \\
& \ddots & & & \ddots & & & \ddots & & \cdots & & \ddots & & \vdots \\
& & 1 & & & 1 & & & 2 & & & & q-1 & 0 \\
0 & \cdots & 0 & 1 & \cdots & 1 & 1 & \cdots & 1 & & 1 & \cdots & 1 & 1
\end{bmatrix}.$$

All unmarked entries are zeroes. From the results presented in Section 5, the following lengthening theorem is then obtained.

Theorem 12 *If q is a prime power, then $K_q(qn+1,R) \le q^{n(q-1)} K_q(n,R)$.*

For q a prime and $R=1$, this theorem was proved in [4]; it was later generalized to prime powers and arbitrary radii in [63]. In [16] a proof of the case $q=2$, $R=1$ is given based on another construction found by Mollard and, independently, Katsman and Litsyn; that construction can also be generalized in another way, as shown by Honkala and Hämäläinen [34, 39].

This is a very useful construction for $R=1$. For example, for a fixed q, starting from the Hamming code of length $q+1$, a series of codes is obtained with the same parameters as the q-ary Hamming codes by repeatedly applying the construction that proves Theorem 12. Unfortunately, the construction cannot easily be generalized to arbitrary covering radii. In [37], however, Honkala uses some results about finite fields to develop a lengthening construction that works efficiently in many cases where $R > 1$, generalizing many earlier results including Theorem 12 for q a prime and some results in [4]. The construction proves the following theorem.

Theorem 13 *If q is a prime, then $K_q(tn+1,R) \leq sq^{(t-1)n}K_q(n,R)$, where $s = \max\{1, q-(t-1)R\}$.*

Upper bounds that this theorem leads to can be found in [4, 37]. For q a prime power, Honkala gives similar constructions in [37]. These lengthening constructions cannot be efficiently generalized to codes over mixed alphabets.

7 Conclusions

In this thesis construction methods (occasionally in the form of upper bounds that are proved by the constructions) for covering codes are presented. The new results in [P1] to [P6] are surveyed and related to earlier results on this problem. The use of computers has played a central role in the research; many of the methods presented are based on computer search. Simulated annealing has turned out to perform very well in many cases. Although a new code that is found in such a search is not as valuable as if it were proved mathematically, such proofs can many times be found by investigating the code found in the search. Examples of this are the ternary covering codes of length 8 and 11 that are treated in [56] and [P5], respectively.

In all papers [P1] to [P6] not only construction methods are presented but also record-breaking upper bounds that these methods lead to. The following extensive tables of upper bounds can be found in the publications: [P2]: $K_3(n,R)$ for $n \leq 14$, $R \leq 9$, $K_4(n,R)$ for $n \leq 10$, $R \leq 7$, and $K_5(n,R)$ for $n \leq 9$, $R \leq 7$; [P4]: $K_{5,4,3,2}(n_1,n_2,n_3,n_4;R)$ for $n_1+n_2+n_3+n_4 \leq 4$, $R \leq 3$; [P5]: $K_3(n,1)$ for $n \leq 14$; and [P6]: $K_{3,2}(n_1,n_2;R)$ for $n_1+n_2 \leq 13$, $R \leq 3$.

As for applications of covering codes, the possibility of using them as football pool systems was already mentioned; this is also the main application. Other possible applications include distribution of resources in hypercube computers [65] and coding of speech [24]. A number of other applications of covering codes in different problems of information theory and computer science are mentioned, for example, in [15].

References

[1] E. Aarts and J. Korst, "Simulated Annealing and Boltzmann Machines: A Stochastic Approach to Combinatorial Optimization and Neural Computing," Wiley, Chichester, 1989.

[2] E. Balas and A. Ho, Set covering algorithms using cutting planes, heuristics and subgradient optimization: a computational study, *Math. Programming* **12** (1980), 37–60.

[3] J. E. Beasley, An algorithm for set covering problem, *European J. Oper. Res.* **31** (1987), 85–93.

[4] A. Blokhuis and C. W. H. Lam, More coverings by rook domains, *J. Combin. Theory Ser. A* **36** (1984), 240–244.

[5] 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* **36** (1990), 1334–1380.

[6] R. A. Brualdi, V. S. Pless, and R. M. Wilson, Short codes with a given covering radius, *IEEE Trans. Inform. Theory* **35** (1989), 99–109.

[7] R. A. Brualdi and V. S. Pless, On the length of codes with a given covering radius, in D. Ray-Chauduri (ed.), "Coding Theory and Design Theory. Part I: Coding Theory," Springer-Verlag, New York, 1990, pp. 9–15.

[8] A. R. Calderbank and N. J. A. Sloane, Inequalities for covering codes, *IEEE Trans. Inform. Theory* **34** (1988), 1276–1280.

[9] W. A. Carnielli, On covering and coloring problems for rook domains, *Discrete Math.* **57** (1985), 9–16.

[10] W. A. Carnielli, Hyper-rook domain inequalities, *Stud. Appl. Math.* **82** (1990), 59–69.

[11] V. Černy, Thermodynamical approach to the traveling salesman problem: an efficient simulation algorithm, *J. Opt. Theory Appl.* **45** (1985), 41–51.

[12] W. Chen and I. S. Honkala, Lower bounds for q-ary covering codes, *IEEE Trans. Inform. Theory* **36** (1990), 664–671.

[13] N. Christofides and S. Korman, A computational survey of methods for the set covering problem, *Management Sci.* **21** (1975), 591–599.

[14] R. F. Clayton, "Multiple Packings and Coverings in Algebraic Coding Theory," Ph.D. thesis, Univ. of California Los Angeles, 1987.

[15] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, Covering radius—survey and recent results, *IEEE Trans. Inform. Theory* **31** (1985), 328–343.

[16] G. D. Cohen, A. C. Lobstein, and N. J. A. Sloane, Further results on the covering radius of codes, *IEEE Trans. Inform. Theory* **32** (1986), 680–694.

[17] T. J. Dickson, On a covering problem concerning Abelian groups, *J. London Math. Soc. (2)* **3** (1971), 222–232.

[18] A. A. El Gamal, L. A. Hemachandra, I. Shperling, and V. K. Wei, Using simulated annealing to design good codes, *IEEE Trans. Inform. Theory* **33** (1987), 116–123.

[19] J. Etcheberry, The set-covering problem: a new implicit enumeration algorithm, *Oper. Res.* **25** (1977), 760–772.

[20] T. Etzion and G. Greenberg, Constructions for perfect mixed codes and other covering codes, *IEEE Trans. Inform. Theory* **39** (1993), 209–214.

[21] H. Fernandes and E. Rechtschaffen, The football pool problem for 7 and 8 matches, *J. Combin. Theory Ser. A* **35** (1983), 109–114.

[22] A. B. Fontaine and W. W. Peterson, Group code equivalence and optimum codes, *IEEE Trans. Inform. Theory* **5** (Special Supplement) (1959), 60–70.

[23] S. W. Golomb and E. C. Posner, Rook domains, Latin squares, affine planes, and error-distributing codes, *IEEE Trans. Inform. Theory* **10** (1964), 196–208.

[24] R. L. Graham and N. J. A. Sloane, On the covering radius of codes, *IEEE Trans. Inform. Theory* **31** (1985), 385–401.

[25] H. O. Hämäläinen, I. S. Honkala, M. K. Kaikkonen, and S. N. Litsyn, Bounds for binary multiple covering codes, *Des. Codes Cryptogr.* **3** (1993), 251–275.

[26] H. O. Hämäläinen, I. S. Honkala, and S. N. Litsyn, Bounds for binary codes that are multiple coverings of the farthest-off points, submitted for publication.

[27] H. Hämäläinen and S. Rankinen, Upper bounds for football pool problems and mixed covering codes, *J. Combin. Theory Ser. A* **56** (1991), 84–95.

[28] O. Heden, A generalized Lloyd theorem and mixed perfect codes, *Mathematica Scand.* **37** (1975), 13–26.

[29] O. Heden, A new construction of group and nongroup perfect codes, *Inform. and Control* **34** (1977), 314–323.

[30] M. Herzog and J. Schönheim, Group partition, factorization and the vector covering problem, *Canad. Math. Bull.* **15** (1972), 207–214.

[31] M. Herzog and J. Schönheim, Linear and nonlinear single-error-correcting perfect mixed codes, *Inform. and Control* **18** (1971), 364–368.

[32] I. S. Honkala, Lower bounds for binary covering codes, *IEEE Trans. Inform. Theory* **34** (1988), 326–329.

[33] I. S. Honkala, On the normality of codes with covering radius one, in "Proc. Fourth Joint Swedish-Soviet Int. Workshop Inform. Theory," Studentlitteratur, Lund, 1989, pp. 223–226.

[34] I. S. Honkala, Modified bounds for covering codes, *IEEE Trans. Inform. Theory* **37** (1991), 351–365.

[35] I. S. Honkala, On (k,t)-subnormal covering codes, *IEEE Trans. Inform. Theory* **37** (1991), 1203–1206.

[36] I. S. Honkala, All binary codes with covering radius one are subnormal, *Discrete Math.* **94** (1991), 229–232.

[37] I. S. Honkala, On lengthening of covering codes, *Discrete Math.* **106/107** (1992), 291–295.

[38] I. Honkala, On $(q,1)$-subnormal q-ary covering codes, *Discrete Appl. Math.*, to appear.

[39] I. S. Honkala and H. O. Hämäläinen, A new construction for covering codes, *IEEE Trans. Inform. Theory* **34** (1988), 1343–1344.

[40] I. S. Honkala and H. O. Hämäläinen, Bounds for abnormal binary codes with covering radius one, *IEEE Trans. Inform. Theory* **37** (1991), 372–375.

[41] X. Hou, Some results on the norm of codes, *IEEE Trans. Inform. Theory* **36** (1990), 683–685.

[42] X. Hou, New lower bounds for covering codes, *IEEE Trans. Inform. Theory* **36** (1990), 895–899.

[43] X. Hou, An improved sphere covering bound for the codes with $n = 3R+2$, *IEEE Trans. Inform. Theory* **36** (1990), 1476–1478.

[44] X. Hou, Binary linear quasi-perfect codes are normal, *IEEE Trans. Inform. Theory* **37** (1991), 378–379.

[45] G. A. Kabatyanskii and V. I. Panchenko, Unit sphere packings and coverings of the Hamming space, *Problemy Peredachi Informatsii* **24** (1988), 3–16 (in Russian; English translation in *Problems Inform. Transmission* **24** (1988), 261–272).

[46] J. G. Kalbfleisch and R. G. Stanton, A combinatorial problem in matching, *J. London Math. Soc.* (*1*) **44** (1969), 60–64; and (*2*) **1** (1969), 398.

[47] J. G. Kalbfleisch, R. G. Stanton, and J. D. Horton, On covering sets and error-correcting codes, *J. Combin. Theory* **11** (1971), 233–250.

[48] J. G. Kalbfleisch and P. H. Weiland, Some new results for the covering problem, in W. T. Tutte (ed.), "Recent Progress in Combinatorics," Academic Press, New York, 1969, pp. 37–45.

[49] H. J. L. Kamps and J. H. van Lint, The football pool problem for 5 matches, *J. Combin. Theory* **3** (1967), 315–325.

[50] H. J. L. Kamps and J. H. van Lint, A covering problem, in "Colloq. Math. Soc. János Bolyai; Hung. Combin. Theory and Appl.," Balantonfüred, Hungary, 1969, pp. 679–685.

[51] K. E. Kilby and N. J. A. Sloane, On the covering radius problem for codes I. Bounds on normalized covering radius, *SIAM J. Alg. Discr. Meth.* **8** (1987), 604–618.

[52] K. E. Kilby and N. J. A. Sloane, On the covering radius problem for codes II. Codes of low dimension; normal and abnormal codes, *SIAM J. Alg. Discr. Meth.* **8** (1987), 619–627.

[53] S. Kirkpatrick, C. D. Gelatt Jr., and M. P. Vecchi, Optimization by simulated annealing, *Science* **220** (1983), 671–680.

[54] E. Kolev, Codes over GF(3) of length 5, 27 codewords and covering radius 1, submitted for publication.

[55] P. J. M. van Laarhoven and E. H. L. Aarts, "Simulated Annealing: Theory and Applications," Reidel, Dordrecht, 1987.

[56] 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, *J. Combin. Theory Ser. A* **52** (1989), 304–312.

[57] H. W. Lenstra Jr., Two theorems on perfect codes, *Discrete Math.* **3** (1972), 125–132.

[58] D. Li and W. Chen, New lower bounds for binary covering codes, submitted for publication.

[59] B. Lindström, Group partitions and mixed perfect codes, *Canad. Math. Bull.* **18** (1975), 57–60.

[60] J. H. van Lint, A survey of perfect codes, *Rocky Mountain J. Math.* **5** (1975), 199–224.

[61] J. H. van Lint, "Introduction to Coding Theory," Springer-Verlag, New York, 1982.

[62] J. H. van Lint, Recent results on covering problems, in T. Mora (ed.), "Applied Algebra, Algebraic Algorithms and Error-Correcting Codes," LNCS 357, Springer-Verlag, Berlin, 1989, pp. 7–21.

[63] J. H. van Lint Jr., "Covering Radius Problems," M.Sc. thesis, Eindhoven University of Technology, The Netherlands, June 1988.

[64] J. H. van Lint Jr. and G. J. M. van Wee, Generalized bounds on binary/ternary mixed packing- and covering codes, *J. Combin. Theory Ser. A* **57** (1991), 130–143.

[65] M. Livingston and Q.F. Stout, Distributing resources in hypercube computers, in G. Fox (ed.), "Proc. of the Third Conference on Hypercube Multiprocessors," Pasadena, 1988, pp. 222-231.

[66] A. C. Lobstein and G. J. M. van Wee, On normal and subnormal q-ary covering codes, *IEEE Trans. Inform. Theory* **35** (1989), 1291–1295; and **36** (1990), 1498.

[67] G. O. Losey, Note on a theorem of Zaremba, *J. Combin. Theory* **6** (1969), 208–209.

[68] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.

[69] E. Mattioli, Sopra una particolare proprieta dei gruppi abeliani finiti, *Ann. Scuola Norm. Sup. Pisa (3)* **3** (1950), 59–65.

[70] J. G. Mauldon, Covering theorems for groups, *Quart J. Math. Oxford (2)* **1** (1950), 284–287.

[71] V. I. Panchenko, Packings and coverings over an arbitrary alphabet, *Problemy Peredachi Informatsii* **24** (1988), 93–96 (in Russian; English translation in *Problems Inform. Transmission* **24** (1988), 331–333).

[72] C. H. Papadimitriou and K. Steiglitz, "Combinatorial Optimization: Algorithms and Complexity," Prentice-Hall, New York, 1982.

[73] K. T. Phelps, A general product construction for error correcting codes, *SIAM J. Alg. Discr. Meth.* **5** (1984), 224–228.

[74] V. Pless, "Introduction to the Theory of Error-Correcting Codes," Wiley, New York, 1989.

[75] C. L. M. van Pul and T. Etzion, New lower bounds for constant weight codes, *IEEE Trans. Inform. Theory* **35** (1989), 1324–1329.

[76] E. R. Rodemich, Coverings by rook domains, *J. Combin. Theory* **9** (1970), 117–128.

[77] D. Slepian, Some further theory of group codes, *Bell System Tech. J.* **39** (1960), 1219–1252.

[78] N. J. A. Sloane, A new approach to the covering radius of codes, *J. Combin. Theory Ser. A* **42** (1986), 61–86.

[79] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, New binary codes, *IEEE Trans. Inform. Theory* **18** (1972), 503–510.

[80] R. G. Stanton, Covering theorems in groups (or: How to win at football pools), in W. T. Tutte (ed.), "Recent Progress in Combinatorics," Academic Press, New York, 1969, pp. 21–36.

[81] R. G. Stanton and J. A. Bate, A computer search for B-coverings, in R. W. Robinson, G. W. Southern, and W. D. Wallis (eds.), "Combinatorial Mathematics VII," LNM 829, Springer-Verlag, Berlin, 1980, pp. 37–50.

[82] 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.* **1** (1969), 493–499.

[83] R. G. Stanton and J. G. Kalbfleisch, Covering problems for dichotomized matchings, *Aequationes Math.* **1** (1968), 94–103.

[84] R. G. Stanton and J. G. Kalbfleisch, Intersection inequalities for the covering problem, *SIAM J. Appl. Math.* **17** (1969), 1311–1316.

[85] P. Tannenbaum, Partitions of Z_2^n, *SIAM J. Alg. Discr. Meth.* **4** (1983), 22–29.

[86] O. Taussky and J. Todd, Covering theorems for groups, *Ann. Soc. Polon. Math.* **21** (1948), 303–305.

[87] O. Taussky and J. Todd, Some discrete variable computations, *Proc. Sympos. Appl. Math.* **10** (1960), 201–209.

[88] H. N. Ward, A form for M_{11}, *J. Alg.* **37** (1975), 340–361.

[89] E. W. Weber, On the football pool problem for 6 matches: a new upper bound, *J. Combin. Theory Ser. A* **35** (1983), 106–108.

[90] G. J. M. van Wee, Improved sphere bounds on the covering radius of codes, *IEEE Trans. Inform. Theory* **34** (1988), 237–245.

[91] G. J. M. van Wee, More binary covering codes are normal, *IEEE Trans. Inform. Theory* **36** (1990), 1466–1470.

[92] G. J. M. van Wee, Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces, *J. Combin. Theory Ser. A* **57** (1991), 117–129.

[93] G. J. M. van Wee, On the non-existence of certain perfect mixed codes, *Discrete Math.* **87** (1991), 323–326.

[94] G. J. M. van Wee, "Covering Codes, Perfect Codes, and Codes from Algebraic Curves," Ph.D. thesis, Eindhoven University of Technology, The Netherlands, June 1991.

[95] 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* **37** (1991), 678–682.

[96] G. J. M. van Wee, Some new lower bounds for binary and ternary covering codes, *IEEE Trans. Inform. Theory*, to appear.

[97] L. T. Wille, The football pool problem for 6 matches: a new upper bound obtained by simulated annealing, *J. Combin. Theory Ser. A* **45** (1987), 171–177.

[98] S. K. Zaremba, A covering theorem for Abelian groups, *J. London Math. Soc.* **26** (1950), 71–72.

[99] S. K. Zaremba, Covering problems concerning Abelian groups, *J. London Math. Soc.* **27** (1952), 242–246.

[100] Z. Zhang, Linear inequalities for covering codes: Part I—pair covering inequalities, *IEEE Trans. Inform. Theory* **37** (1991), 573–582.

[101] Z. Zhang and C. Lo, Lower bounds on $t[n, k]$ from linear inequalities, *IEEE Trans. Inform. Theory* **38** (1992), 194–197.

[102] Z. Zhang and C. Lo, Linear inequalities for covering codes: Part II—triple covering inequalities, *IEEE Trans. Inform. Theory* **38** (1992), 1648–1662.

Errata

Paper [P2]:

Appendix A	The $(5,5,35)2$ code: 41103 should read 41403.

Paper [P4]:

Theorem 9	The case $\mathrm{ms}_{5,6,6,6}(1,1,1,1;2) = 36$ must be included in the proof.

Paper [P6]:

Theorem 5	Should read: … *linear* perfect covering….
Theorem 9	The $(3,2;4,1;18)1$ code in Table III is not strongly semi-normal, and Theorem 9 should be deleted. However, the partitioned code has the strong property that for any $x \in F_3^4 F_2^1$, $\sum_i d(x, C_i) \leq 5$, and Theorem 9 has been checked to hold for the cases in Table II where it is used.
Theorem 16	Page 12, line 10 should read $\ldots, x \in F_2^{11}, \ldots$.