Weighted Coverings and Packings

G. D. Cohen

Iiro Honkala

S. N. Litsyn

H. F. Mattson Jr

Recommended Citation

SU-CIS-95-1

Weighted Coverings and Packings

Gérard Cohen, Iiro Honkala
Simon Litsyn, H. F. Mattson, Jr.

February 1995

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

Weighted Coverings and Packings[1]

Gérard Cohen
Ecole Nationale Supérieure des Télécommunications
46 rue Barrault, C-220-5
75634 Paris Cédex 13, France
e-mail: cohen@inf.enst.fr

Iiro Honkala
Department of Mathematics
University of Turku, 20500 Turku 50, Finland
e-mail: honkala@sara.utu.fi

Simon Litsyn[2]
Department of Electrical Engineering Systems
Tel Aviv University, Ramat Aviv, 69978, Israel
e-mail: litsyn@eng.tau.ac.il

H. F. Mattson, Jr.
School of Computer and Information Science
4-116 Center for Science & Technology
Syracuse, New York 13244-4100
e-mail: jen@SUVM.acs.syr.edu

Key words: Combinatorial codes, Coverings, Perfect codes, Constructions of codes.

Abstract

In this paper we introduce a generalization of the concepts of coverings and packings in Hamming space called weighted coverings and packings. This allows us to formulate a number of well-known coding theoretical problems in a uniform manner. We study the existence of perfect weighted codes, discuss connections between weighted coverings and packings, and present many constructions for them.

1 Introduction

Conventional packings and coverings are arrangements of Hamming spheres of a given radius in the Hamming space. We generalize these concepts by attaching weights to different layers of the Hamming sphere. If several such spheres intersect in a point of the space we define the density at that point as the sum of the weights of the corresponding layers. In this paper we study the general problem of weighted packings (coverings) for which the density at each point is at most one (resp. at least one). In this way we can consider several known types of codes, e.g., the uniformly packed codes, list codes, multiple coverings, L-codes, in a uniform way. Some results about this problem have previously been presented in several conferences, see [15, 16, 13]. **The goal** of our paper is to provide an introduction to this interesting area, summarize what is known about it, and state some new results.

There are many applications of weighted packings and coverings. In particular, we would like to mention two. The first is list decoding; see [4],[19] and their references. In list decoding the output of the decoder is a list with a given maximum size, and correct decoding means that the transmitted codeword appears in the list. If the received word is in fact a codeword, we do not actually want to have a long list of possibilities. On the other hand, if the received word is very unreliable, i.e., very far from the code, it would be desirable to have a longer list. So we arrive to the following generalization of list decoding. We want the size of the list to be a function of the Hamming distances between the received word and the codewords. This leads us to weighted packings. This kind of criterion could be useful, for example, in spelling checkers with the code being the English (French, Finnish, Hebrew) vocabulary, and the "ambient" space being all combinations of letters with maximal length n.

For our second application of weighted coverings we consider a generalized football pool problem [28], [32]. A player wishes to forecast the outcome of n football matches (each with three possible outcomes) and is allowed to make several guesses (each guess being a word in $\mathbf{F}_3^n$). A guess with exactly k wrong outcomes wins the player a $(k+1)^{\text{st}}$ prize. If the

player thinks he knows the outcome of some $i \geq 1$ matches he may wish to fix an integer R and construct a set of forecasts in such a way that, no matter what the outcomes in the remaining $n - i$ matches, he will win at least an $(R + 1)^{\text{st}}$ prize (provided he is right about the i matches). In other words, he wishes to construct a code $C \subseteq \mathbf{F}_3^{n-i}$ with covering radius at most R. If he instead uses a μ-fold covering code, defined as a weighted covering with the same weight $1/\mu$ attached to the first $R + 1$ layers (i.e., the vectors at distances $0, 1, \ldots, R$ from C), he will be guaranteed to win the $(R + 1)^{\text{st}}$ prize at least μ times (more precisely, he will win at least μ prizes each of which is at least the $(R + 1)^{\text{st}}$ prize). Such codes are called *multiple coverings* (MC). However, the player wants to surely win a certain amount of money, so it is natural to attach different weights to different prizes and construct a weighted covering instead. For that purpose *multiple coverings of the farthest-off points* (MCF) are introduced in [26]. For constructions and numerical tables for binary MC and MCF, see [25],[27] and [26]. Let us give an illustration.

Example 1.1 Suppose $n = 13$, $i = 9$. Furthermore, assume that the player is able to exclude one of the outcomes in each of the remaining four matches. He wishes to find a suitable set of forecasts that—no matter what the outcomes in the remaining four matches are—ensures him a forecast in which there is at most one incorrect result. Then he can use the following four forecasts (after choosing a suitable notation for the outcomes):

$$C_1 = \{0000, \ 0111, \ 1000, \ 1111\}.$$

If the player uses the four forecasts of C_1 twice, he is guaranteed to get at least two forecasts with at most one incorrect entry. The same can be achieved using C_2, $7 = |C_2| < 2|C_1|$, where

$$C_2 = \{0001, \ 0010, \ 0011, \ 1100, \ 1100, \ 0111, \ 1011\}.$$

However, by using only the following *six* forecasts of C_3

$$C_3 = \{1111, \ 1111, \ 1000, \ 0100, \ 0010, \ 0001\},$$

he will always get at least one entirely correct forecast or at least two forecasts with one incorrect entry, as can easily be checked.

C_1, C_2 and C_3 are weighted coverings with weights $\{1, 1\}$, $\{1/2, 1/2\}$ and $\{1, 1/2\}$ resp. attached to the first two layers.

Weighted coverings are also used to prove lower bounds on the cardinality of binary codes with a given length and covering radius (see [40], [41], [31]): one shows that such a code

2

is a weighted covering for a suitable collection of weights and then uses the sphere-covering lower bound for weighted coverings. Weighted coverings can be found in [20] as well, in a construction for mixed perfect codes.

From now on, we study only *codes* in this paper, i.e, the same word is never allowed to appear more than once.

The paper is organized as follows. In Section 2 we introduce the notations and present a unified approach to previous work. Section 3 is devoted to a strong necessary condition for the existence of perfect weighted coverings (PWC), the Lloyd theorem. In Section 4 we classify all q-ary linear PWC with radius one. In Section 5 we study a subcase of PWC, namely linear perfect multiple coverings (PMC) of radius 2, according to the number of distances s of the dual code. The case $s = 1$ is settled; for $s = 2$, we conjecture that we have found all existing codes with minimum distance two. Section 6 establishes connections between weighted packings and coverings, showing their complementarity. Section 7 presents a number of constructions for weighted coverings and packings.

2   Notations and known results

We denote by $\mathbf{F}_q$ the q-ary alphabet. If q is 2, we usually omit it. Denote by $\mathbf{F}^n$ the vector space of binary n-tuples, by $d(\cdot, \cdot)$ the Hamming distance, by $C(n, K, d)R$ a code C with length n, size K, minimum distance $d = d(C)$ and covering radius $R = R(C)$. When C is linear, we write $C[n, k, d]R$, where k is the binary log of K (or simply $[n, k]R$ or $[n, k]$). We denote the Hamming weight of $x \in \mathbf{F}^n$ by $wt(x)$.

For $x \in \mathbf{F}^n$, $A(x) = (A_0(x), A_1(x) \ldots A_n(x))$ 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 $M = (m_0, m_1, \ldots, m_n)$ of weights, i.e., rational numbers, we define the *M-density* of C at x as
$$\theta(x) := \sum_{i=0}^{n} m_i \, A_i(x) = <M, A(x)>. \tag{2.1}$$

We say that a code C is an *M-covering* if
$$\theta(x) \geq 1$$
for all $x \in \mathbf{F}^n$, and it is an *M-packing* if
$$\theta(x) \leq 1$$

for all $x \in \mathbf{F}^n$. Furthermore, C is a *perfect M-covering (PWC)* if $\theta(x) = 1$ for all $x \in \mathbf{F}^n$. We define the *radius* of an M-covering as

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

From now on we always assume that all codes are binary unless otherwise stated. Here are the known special cases:

- Classical codes and coverings: $m_i = 1$ for $i = 0, 1, \ldots, \delta$.

- List codes [4], [19] and multiple coverings [11], [25]: $m_i = 1/j$ where j is a positive integer, for $i = 0, 1, \ldots, \delta$.

- Multiple coverings of the farthest-off points (MCF) [26]: $m_i = 1$ for $i = 0, 1, \ldots, \delta - 1, m_\delta = 1/j$, where j is a positive integer.

Many known classes of codes can be viewed as perfect weighted coverings:

- Classical perfect codes [35]: $m_i = 1$ for $i = 0, 1, \ldots \delta$.

- Nearly perfect codes [21], [37]: $m_i = 1$ for $i = 0, 1, \ldots, e - 1, m_e = m_{e+1} = 1/[(n + 1)/(e + 1)]$, where $e = [(d-1)/2]$.

- Perfect multiple coverings (PMC) [39] and [11]: $m_i = 1/j$ for $i = 0, 1, \ldots \delta$, where j is a positive integer.

- Perfect L-codes [30] and [12] : $m_i = 1$ for $i \in L \subseteq \{0, 1, \ldots, \lfloor n/2 \rfloor\}$.

- Strongly uniformly packed codes [37], [8]:

$$m_i = 1 \text{ for } i = 0, 1, \ldots, e - 1, \ m_e = m_{e+1} = 1/r \, ;$$

  for some integer r.

- Uniformly packed codes of j-th order [22]:

$$m_i = 1 \text{ for } i = 0, 1, \ldots, d - e - j - 1;$$

$$m_i = 1 - t/r \text{ for } d - e - j \leq i \leq e;$$

$$m_i = 1/r \text{ for } e + 1 \leq i \leq e + j,$$

  for t and r integers.

4

- Uniformly packed codes [7], [22]: $\delta(M) = R(C)$.

It can be shown that every code is a PWC with respect to a suitable weight vector M. In fact, suppose that C is a linear code and that the number of non-zero weights in the dual code of C is s. Then, by a result of Delsarte [18] one can always choose $\delta = s$:

Proposition 2.1 *A code C is a perfect M-covering with $\delta(M) = s$. In that case the m_i's are uniquely determined by*

$$m_i = \alpha_i, \quad 0 \le i \le s,$$

where α_i is the ith coefficient in the Krawtchouk expansion of the annihilator polynomial $\alpha(x)$ of C. Here

$$\alpha(x) := 2^{n-k} \prod_{w \in W} \left(1 - \frac{x}{w}\right),$$

and W is the set of s nonzero weights of vectors in $C^{\perp}$.

So, in our notation, a uniformly packed code in the sense of [7] is just a PWC with $\delta(M) = R(C)$. In that case, $R = s = \delta$ and Proposition 2.1 applies. The reason is that $R \le s \le \delta$ in general. The first inequality is Delsarte's Theorem, (3.3) of [18]; the second is Corollary 3.1. A similar remark applies to non-linear codes as well.

Another example could be found if δ is permitted to be as large as n. Then every code C can be viewed as a PWC with $m_i = 1/|C|$ for all $i = 0, 1, \ldots, n$.

Nevertheless, we are interested in a different problem: given a weight vector M, we would like to determine for which lengths there exist PWC, or to provide good weighted packings and coverings. Notice that the same code can be a PWC for different weight vectors if $\delta(M) > s$ (consider for example $C = \mathbf{F}^n$).

It is interesting to draw some parallels with design theory [3]. In design theory (where the covering relation is set-theoretic inclusion) we are interested not only in Steiner systems, t-designs and covering and packing designs, but also in more general configurations like in [9] . Similarly, we are interested not only in perfect codes, perfect t-fold multiple coverings and covering and packing codes but also in more general codes like the weighted coverings.

If C is an M-covering one gets from the definition:

$$\sum_{i=0}^{n} m_i A_i(x) \ge 1 \text{ for all } x.$$

Summing over all x in $\mathbf{F}^n$ and permuting sums, we get

$$\sum_{i=0}^{n} m_i \sum_{x \in \mathbf{F}^n} A_i(x) \ge 2^n.$$

5

For $i = 0$, the second sum is $|C| = K$, for $i = 1$ it is Kn, and so on. Therefore we get the following *sphere-covering lower bound* on weighted coverings:

$$K \sum_{i=0}^{n} m_i \binom{n}{i} \geq 2^n . \tag{2.2}$$

Similarly, we see that if C is a weighted M-packing then

$$K \sum_{i=0}^{n} m_i \binom{n}{i} \leq 2^n . \tag{2.3}$$

In particular, for the perfect M-covering C we get the the following analog of the Hamming condition.

Proposition 2.2 *A covering C is a perfect M-covering if and only if*

$$K \sum_{i=0}^{n} m_i \binom{n}{i} = 2^n . \tag{2.4}$$

□

We can interpret (2.4) in a geometrical way: we define a weighted sphere around any vector c in $\mathbf{F}^n$ by means of the function

$$\omega_c(x) := m_{d(c,x)}. \tag{2.5}$$

For $d(c, x) > \delta$, $\omega_c(x) = 0$; hence δ can be viewed as the radius of the weighted sphere, denoted by $S(c, \delta)$. Set

$$\omega(S(c,\delta)) := \sum_{x} \omega_c(x) = \sum_{i=0}^{n} m_i \binom{n}{i};$$

then (2.5) becomes

$$\omega(S(c,\delta)) = 2^n/K$$

so that C is a *perfect weighted covering* (PWC) of $\mathbf{F}^n$.

Equation (2.5) is reminiscent of a *fuzzy membership* function, as studied, e.g., in [5].

In the next sections we will attempt to classify the perfect weighted coverings of small radius.

3   A Lloyd theorem

In his new proof of Lloyd's theorem[3] [34] in 1965–1966, A. M. Gleason introduced the group algebra into coding theory. Since Gleason did not publish his proof, but left it to be recorded in [2], many coding theorists may never have seen it. We found that it extended effortlessly to the present setting, and we thus present it here, specialized, for simplicity, to the binary case. (Gleason proved the result for general prime powers q; evidently, his method yields a q-ary version of Theorems 3.1 and 3.2.) We are grateful to a referee for pointing out that our Lloyd theorem can also be proved by appealing to work of Delsarte showing that his annihilator polynomial divides the Lloyd polynomial. But for completeness and for historical interest, we prefer to present the following proof.

We denote by $P_{n,i}(x)$ the Krawtchouk polynomial, for $0 \leq i \leq n$,

$$P_{n,i}(x) = \sum_{0 \leq j \leq i} (-1)^j \binom{n-x}{i-j} \binom{x}{j}. \tag{3.1}$$

Theorem 3.1 *Let C be a perfect weighted covering with $M = (m_0, m_1, \ldots, m_\delta)$ and covering radius R. Then the Lloyd polynomial of this covering,*

$$L(x) := \sum_{0 \leq i \leq \delta} m_i\, P_{n,i}(x)$$

has at least R distinct integral roots among $1, 2, \ldots, n$.

In the linear case we have

Theorem 3.2 *An $[n, k, d]\, R$ code C is a perfect $(m_0, m_1, \ldots, m_\delta)$-covering only if the Lloyd polynomial*

$$L(x) := \sum_{0 \leq i \leq \delta} m_i\, P_{n,i}(x)$$

has among its roots the s nonzero weights of $C^{\perp}$.

Corollary 3.1 $s \leq \delta$.

Proof of Theorem 3.1. (Adapted from Gleason's proof in [2], Chapter II, Section 1) We use the group algebra $\mathcal{A}$ of all formal polynomials

$$\sum_{a \in \mathbf{F}^n} \gamma_a X^a$$

---

[3]Golay [23] anticipated Lloyd's theorem in the linear case.

with $\gamma_a \in \mathbf{Q}$, the field of rational numbers.

Define

$$S := \sum_{0 \le i \le \delta} m_i \sum_{wt(a)=i} X^a. \tag{3.2}$$

We let the symbol C for our code also stand for the corresponding element in $\mathcal{A}$, namely,

$$C := \sum_{c \in C} X^c. \tag{3.3}$$

Then we find that

$$SC = \sum_{c \in C} X^c \cdot S = \mathbf{F}^n := \sum_{a \in \mathbf{F}^n} X^a. \tag{3.4}$$

Characters on $\mathbf{F}^n$ are group homomorphisms of $(\mathbf{F}^n, +)$ into $\{1, -1\}$, the group of order 2 in $\mathbf{Q}^*$. All characters have the form χ_u for $u \in \mathbf{F}^n$, where χ_u is defined as

$$\chi_u(v) = (-1)^{u \cdot v} \quad \text{for} \quad u, v \in \mathbf{F}^n.$$

We use linearity to extend χ_u to a linear functional defined on $\mathcal{A}$: For all $Y \in \mathcal{A}$

$$\text{if } Y = \sum_{a \in \mathbf{F}^n} \gamma_a X^a, \text{ then } \chi_u(Y) := \sum \gamma_a \chi_u(a).$$

It follows that

$$\chi_u(YZ) = \chi_u(Y)\chi_u(Z) \quad \text{for all } Y, Z \in \mathcal{A}.$$

It is known [2], [18] that for any $u \in \mathbf{F}^n$, if $wt(u) = w$, then

$$\chi_u \left(\sum_{wt(a)=i} X^a \right) = P_{n,i}(w). \tag{3.5}$$

It follows that

$$\chi_u(S) = L(w). \tag{3.6}$$

From (3.4), furthermore, we see that

$$\chi_u(SC) = \chi_u(S)\chi_u(C) = 0$$

for all $u \ne 0$.

Let $u_0, u_1, \ldots, u_R$ be translate-leaders for C such that $wt(u_i) = i$. Define

$$C_i := X^{u_i} C.$$

Then

$$S\, C_i = \mathbf{F}^n. \tag{3.7}$$

8

Define the **symmetric sub-ring** $\overline{\mathcal{A}}$ of $\mathcal{A}$ as the set of all elements Y of $\mathcal{A}$ in which the coefficient of X^a depends only on the weight of a:

$$Y = \sum_{a \in \mathbf{F}^n} \gamma_a \, X^a \in \overline{\mathcal{A}} \quad \text{iff} \quad \forall a, b \in \mathbf{F}^n, \; wt(a) = wt(b) \rightarrow \gamma_a = \gamma_b. \tag{3.8}$$

The mapping $T : \mathcal{A} \to \overline{\mathcal{A}}$ defined by

$$T(Y) := \frac{1}{n!} \sum_\varphi \varphi(Y),$$

where φ runs over all $n!$ permutations of the n coordinates of $\mathbf{F}^n$, maps $\overline{\mathcal{A}}$ onto $\overline{\mathcal{A}}$. Furthermore,

$$\forall Y \in \overline{\mathcal{A}}, \; \forall Z \in \mathcal{A}, \; T(YZ) = YT(Z). \tag{3.9}$$

Define $\overline{C}_i := T(C_i)$. Applying (3.9) to (3.7), we see that

$$S\overline{C}_i = \mathbf{F}^n$$

since, of course, $S \in \overline{\mathcal{A}}$. Define also

$$\mathcal{K} := \{Z; \; Z \in \overline{\mathcal{A}}, \; SZ = 0\}. \tag{3.10}$$

Thus $\mathcal{K}$ is the kernel of the linear mapping from $\overline{\mathcal{A}}$ to $\overline{\mathcal{A}}$ defined by $Y \longmapsto SY$ for all $Y \in \overline{\mathcal{A}}$.

It now follows that for any character χ_u such that $\chi_u(S) \neq 0$,

$$\forall Z \in \mathcal{K}, \; \chi_u(Z) = 0.$$

Since $\overline{\mathcal{A}}$ has dimension $n + 1$, its space of linear functionals also has dimension $n + 1$. Since every linear functional on $\overline{\mathcal{A}}$ can be extended to one on $\mathcal{A}$, the $n + 1$ linear functionals on $\overline{\mathcal{A}}$ obtained by restricting the χ_u to $\overline{\mathcal{A}}$, as

$$\chi_u\big|_{\overline{\mathcal{A}}} =: \chi_w \quad \text{for} \quad wt(u) = w$$

$$w = 0, 1, \ldots, n,$$

are linearly independent.

Suppose that ρ is the exact number of values of $w \in \{0, 1, \ldots, n\}$ for which

$$\chi_w(S) \neq 0.$$

9

Since $\chi_w(S)\chi_w(\mathcal{K}) = 0$ for all w, it follows that $\chi_w(\mathcal{K}) = 0$ for ρ values of w. Since $S\overline{C}_i = \mathbf{F}^n$ for $i = 0, 1, \ldots, R$, we see that

$$S(\overline{C}_i - \overline{C}_0) = 0 \quad \text{for} \quad i = 1, \ldots, R.$$

The elements $\overline{C}_i - \overline{C}_0$ are linearly independent because $\overline{C}_i$ contains elements of weight i but of no smaller weight. We find that

$$R \leq \dim_{\mathbf{Q}} \mathcal{K} \leq n + 1 - \rho,$$

since $\mathcal{K}$ is included in the intersection of the t kernels of the χ_w mentioned above. But $n + 1 - \rho$ is the number of χ_w's which vanish on S; therefore $\chi_w(S) = 0$ for at least R values of w.

Notice now that

$$\chi_w(S) = \sum_{0 \leq i \leq \delta} m_i \, P_{n,i}(w).$$

This finishes the proof. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\square$

Remark 3.1 As one can see in the proof of Theorem 3.1 we actually get a slightly stronger result in the non-linear case, namely that the number of zeros of the Lloyd polynomial is at least the number of values $w \in \{0, 1, \ldots, n\}$ for which $\chi_w(S) = 0$, i.e., at least s, the number of non-zero elements in the MacWilliams transform of the distance distribution of the code. In the linear case s equals the number of non-zero weights in $C^{\perp}$.

In case we do not know the covering radius R in Theorem 3.1 we may use for instance the sphere covering lower bound on R.

4 PWC with radius 1

4.1 The linear case

Assume that $\mathbf{F}_q$ is the finite field of q elements. We first give a completely elementary way of determining all the parameters for which a q-ary PWC with radius 1 exists. In the proof we use the concatenation construction, which is also useful in constructing many binary nonlinear PWC. Using results from the previous section and the literature we then show that we can completely characterize all the q-ary linear PWC with radius 1.

If C is an (m_0, m_1)-covering and $C \neq \mathbf{F}_q^n$, then $m_1 > 0$; otherwise the density at a non-codeword could not be at least 1. If, furthermore, C is a perfect (m_0, m_1)-covering then the

density at a non-codeword equals 1, and $m_1 \leq 1$, and also $m_0 \leq 1$ because the density at any codeword equals 1.

Proposition 4.1 *Assume that the codes $C(\alpha) \subset \mathbf{F}_q^n, \alpha \in \mathbf{F}_Q$, are (perfect) (m_0, m_1)-coverings and that they are disjoint and their union is $\mathbf{F}_q^n$. Assume further that $D \subset \mathbf{F}_Q^N$ is a (perfect) (M_0, M_1)-covering. Then the code*

$$\bigcup_{(x_1, \ldots, x_N) \in D} C(x_1) \oplus \cdots \oplus C(x_N)$$

is a (perfect) $(M_0 - NM_1(1 - m_0), m_1 M_1)$-covering in $\mathbf{F}_q^{Nn}$.

Proof. Suppose $z = (z_1, z_2, \ldots, z_N) \in \mathbf{F}_q^{Nn}$ where each z_i has length n. Because the union of the codes $C(\alpha)$ is the whole space $\mathbf{F}_q^n$, there exists a word $y = (y_1, y_2, \ldots, y_N) \in \mathbf{F}_Q^N$ such that $z \in C(y_1) \oplus \cdots \oplus C(y_N)$.

Assume first that $d(y, D) = 1$. Then there are at least $1/M_1$ words $x = (x_1, \ldots, x_N) \in D$ such that $d(y, x) = 1$, and for each such word x there are at least $1/m_1$ words in $C(x_1) \oplus \cdots \oplus C(x_N)$ that have distance 1 to z.

Assume then that $y \in D$. Then $z \in C(y_1) \oplus \cdots \oplus C(y_N)$, and in each $C(y_i)$ there are at least $(1 - m_0)/m_1$ words that have distance 1 to z_i. Therefore, together there are at least $N(1 - m_0)/m_1$ words in $C(y_1) \oplus \cdots \oplus C(y_N)$ that have distance 1 to z. Furthermore, there are at least $(1 - M_0)/M_1$ words $x \in D$ such that $d(y, x) = 1$, and for each such word x there are again at least $1/m_1$ words in $C(x_1) \oplus \cdots \oplus C(x_N)$ that have distance 1 to z.

In both cases it is easy to check that the $(M_0 - NM_1(1 - m_0), m_1 M_1)$-density at z is at least 1.

If the codes $C(\alpha)$ and D are perfect, then in the previous discussion the estimated numbers of words are exact, and in both cases the $(M_0 - NM_1(1 - m_0), m_1 M_1)$-density at z equals 1. $\square$

Proposition 4.2 *If C is a perfect q-ary (m_0, m_1)-covering, then the code $C \oplus \mathbf{F}_q$ is a perfect $(m_0 - (q - 1)m_1, m_1)$-covering.*

Proof. Let $(x, \alpha), x \in \mathbf{F}_q^n, \alpha \in \mathbf{F}_q$ be arbitrary and denote $D = C \oplus \mathbf{F}_q$.

If $x \in C$, then $(x, \alpha) \in D$ and the words of D that have distance 1 to (x, α) are the $q - 1$ words $(x, \beta) \in D, \beta \neq \alpha$, and the $(1 - m_0)/m_1$ words (y, α) where $y \in C$ and $d(y, x) = 1$.

If $d(x, C) = 1$, then also $d((x, \alpha), D) = 1$ and the words of D that have distance 1 to (x, α) are precisely the $1/m_1$ words (y, α) where $y \in C$ and $d(y, x) = 1$. $\square$

11

If $C \subset \mathbf{F}_q^n$ is a perfect linear (m_0, m_1)-covering with K codewords, then according to the sphere-covering equality we have $(m_0 + (q-1)nm_1)K = q^n$.

The numbers m_0, m_1 are rational numbers and by the discussion preceding Proposition 4.1, $m_0 \leq 1$ and $0 < m_1 \leq 1$. Thus $m_0 = a/t$ and $m_1 = b/t$ for some integers $t > 0, a \leq t, 0 < b \leq t$. Because $C \neq \mathbf{F}_q^n$, there exists a point $x \notin C$, and $\theta(x) = 1$ implies that some multiple of b/t equals one, and hence b divides t. On the other hand, if $x \in C$, then $\theta(x) = 1$ implies that some multiple of b/t equals $1 - a/t$ and hence b divides a. We may therefore assume that $b = 1$.

Theorem 4.1 *A perfect q-ary linear (m_0, m_1)-covering $C \neq \mathbf{F}_q^n$ of length n exists if and only if*

$$m_0 = a/t, m_1 = 1/t \quad \text{for some integers} \quad t > 0, a \leq t$$

and $a \equiv t \pmod{(q-1)}$, and for some integer $i > 0$

$$n = \frac{tq^i - a}{q - 1}.$$

Proof. We have already seen that m_0 and m_1 are as described in the theorem. By the sphere-covering equality we have

$$(a/t + (q-1)n/t)K = q^n$$

and because C is linear, its cardinality K is a power of q, say $q^{n-i}, 0 < i \leq n$, and then $n = (tq^i - a)/(q - 1)$. In particular, $a \equiv t \pmod{(q-1)}$.

To construct such codes, assume first that $a = t$. Then we can in Proposition 4.1 choose

$$C(\alpha) = \{x = (x_1, x_2, \ldots, x_t) \in \mathbf{F}_q^t \mid x_1 + x_2 + \cdots + x_t = \alpha\}$$

for $\alpha \in \mathbf{F}_q$ and

$$D = \quad \text{the } q\text{-ary linear Hamming code of length} \quad (q^i - 1)/(q - 1).$$

Each $C(\alpha)$ is a perfect $(1, 1/t)$-covering and D is a perfect $(1, 1)$-covering. Then the construction of Proposition 4.1 yields a perfect $(1, 1/t)$-covering of length $t(q^i - 1)/(q - 1)$. By the construction and the definitions of $C(\alpha)$ and D it is clear that this code is linear. If a is smaller than t, then $a = t - (q-1)j$ for some integer $j \geq 1$, and we obtain the required perfect $(a/t, 1/t)$-covering of length $j + t(q^i - 1)/(q - 1)$ by applying Proposition 4.2 to this code j times. $\qquad \square$

12

In fact, it is even possible to characterize all the q-ary linear PWC with radius 1. Assume that C is a q-ary linear perfect $(m_0, m_1)-$covering. By Corollary 3.1, $s \leq 1$. If $s = 0$ then $C = \mathbf{F}_q^n$, so assume that $s = 1$. It is well-known, cf. [1], that the generator matrix of $C^\perp$ has the form

$$(G_1, G_2, \ldots, G_t, \mathbf{0}) \tag{4.11}$$

where each G_i is a generator matrix of the i-dimensional simplex code and $\mathbf{0}$ is the i by l zero matrix. It is easy to check that there are two kinds of covering equalities, namely, for the points that have distance 0 and 1 to the code. These two equalities are

$$m_0 + (q - 1)lm_1 = 1$$

$$tm_1 = 1,$$

and we see that C is a PWC with $m_1 = 1/t$ and $m_0 = 1 - (q - 1)l/t$. We have therefore proved the following result.

Theorem 4.2 *For every q, n, m_0, m_1 for which there exists a q-ary perfect linear (m_0, m_1)- covering of length n such a PWC is unique up to equivalence.* □

4.2 The nonlinear *PWC* with radius 1

Let us first give two general constructions.

Proposition 4.3 *If there exists a perfect $(m_0, m_1)-$covering of length n, then there exists a perfect $(m_0, m_1/s)-$covering of length ns.*

Proof. Apply the construction of Proposition 4.1 using the perfect (m_0, m_1)-covering of length n as the outer code and the q-ary $[s, s - 1]$ parity check code as the inner code. □

Proposition 4.4 *If $C_1, C_2, \ldots, C_i$ are disjoint perfect $(m_0, m_1)-$coverings of length n, then their union is a perfect $(m_0/i, m_1/i)$-covering.* □

We cannot characterize all the PWC with radius 1. We can, however, give a partial characterization:

Suppose that $C \subset \mathbf{F}_q^n$ is a perfect (not necessarily linear) (m_0, m_1)-covering of length n. As discussed in the previous section, we may assume that $m_1 = 1/t$ and $m_0 = a/t$ for some integers $t > 0$ and $a \leq t$. The case $m_0 = m_1 = 1/t$ corresponds to the *PMC* case; it is considered in [39].

By (2.4),

$$K(a + (q-1)n) = tq^n. \qquad (4.1)$$

If we instead of linearity assume that q is a prime and t is a power of q, then we still know that K is a power of q, and obtain the following result.

Proposition 4.5 *Assume that q is a prime and $t = q^h$. A perfect $(a/t, 1/t)$−covering $C \subset \mathbf{F}_q^n$ exists if and only if $a \equiv t \pmod{(q-1)}$ and for some integer $i > 0$*

$$n = \frac{tq^i - a}{q - 1}.$$

Furthermore, there exists a linear PWC with these parameters.

Proof. Again K is a power of q, say q^{n-i} where $0 < i \leq n$, and $n = (tq^i - a)/(q-1)$ and $a \equiv t \pmod{(q-1)}$. By Theorem 4.1 there exists a linear PWC with these parameters. $\square$

We would like to point out that for some parameters satisfying (4.1) there is no corresponding code. In the binary nonlinear case we have the following non-existence result.

Proposition 4.6 *If a perfect $(1, 1/t)$-covering $C \subset \mathbf{F}^n$ exists and $n \neq t$, then $n \geq 2t + 1$.*

Proof. If necessary we translate C so that the all-zero word does not belong to C. Then there are exactly t codewords of C of weight 1. Suppose x is any other word of weight 1. Then x is covered by t codewords of C of weight 2, none of which has any 1's in common with the codewords of weight 1. Therefore, $n \geq t + (t+1) = 2t + 1$. $\square$

Example 4.1 If $i \geq 3$ is odd and $t = (2^i + 1)/3$, then $n = 2^i - t$ and $K = t2^{n-i}$ satisfy the equality $K(1 + n/t) = 2^n$. However, because $n = 2t - 1$, no perfect binary $(1, 1/t)$-covering of length n exists by the previous proposition.

5   Linear *PMC* with radius 2 $(m_0 = m_1 = m_2 = 1/j)$

5.1   The case $s = 1$

We begin this section by assuming only that the orthogonal code $C^\perp$ has exactly one nonzero weight, i.e., that $s = 1$. Let C be a binary linear $[n, k, d]$ code.

5.1.1 Description of C

Let w denote the nonzero weight in $C^\perp$. Because $s = 1$, we know [1] that $C^\perp$ is a t-fold repetition of the $[2^i - 1, i]$ simplex code S_i, with l zero coordinates appended, for some $t \geq 1$ and $l \geq 0$. Thus $C^\perp$ consists of all words of the form $c^t 0^l$ for $c \in S_i$ (with the superscripts standing for catenation). Here $i := n - k \geq 1$, and $w = t2^{i-1}$, and $n = t(2^i - 1) + l$.

We will need some further notation, but only for this section:

$$n_i := 2^i - 1$$
$$H_i := S_i^\perp.$$

H_1 is the $[1, 0]$ code, and if $i \geq 2, H_i$ is the Hamming code of length n_i.

The orthogonal code C is therefore the direct product $L \times \mathbf{F}^l$, where L is the code $<L_1, L_2>$ spanned by the subcode

$$L_1 := \{(c_1, \ldots, c_t); c_\mu \in H_i, \ 1 \leq \mu \leq t\}$$

and by the subset L_2 of all vectors of weight 2 in L, namely,

$$L_2 := \{0^{\alpha n_i} u \ 0^{\beta n_i} u \ 0^{\gamma n_i}\} \ \text{ if } t \geq 2$$

for $\alpha + \beta + \gamma = t - 2$ and u any unit vector of length n_i. $L_2 = \emptyset$ if $t = 1$.

If $l > 0$, then $d = 1$; if $l = 0$, then $d = 3$ if $t = 1$ and $d = 2$ if $t \geq 2$. If $i = t = 1$, then L is the $[1, 0]$ code; otherwise $d(L) = 2$ or 3. Most of our focus is on this $[tn_i, k - l]$ code L, where we speak of two coordinate-places as *congruent* if they are congruent mod n_i. For example, the two 1's of a vector of weight 2 in L are in congruent places (reflecting two identical coordinate-places in $C^\perp$ as we have ordered it).

5.1.2 Counting

The results of this Lemma will be helpful.

Lemma 5.1 *(i) The number of vectors of weight 2 in L is $\binom{t}{2}(2^i - 1)$; in C it is $\binom{t}{2}(2^i - 1) + \binom{l}{2}$.*

(ii) For each two incongruent coordinate-places α, β of L, the total number of vectors of weight 3 in L with 1's at α and β is t.

(iii) For each coordinate-place α of L, there are exactly $(n_i - t)t/2 = t^2(2^{i-1} - 1)$ vectors of weight 3 in L with a 1 at α.

We omit the proofs, remarking only that we used (*ii*) to prove (*iii*).

We now use Lemma 5.1 to count how many codewords of C are within distance 2 of a given vector.

Let $x \in L$ and $f \in \mathbf{F}^l$. Then $(x; f) \in C$. It is obvious that there are exactly

$$N := 1 + l + \binom{t}{2}(2^i - 1) + \binom{l}{2} \tag{5.1}$$

vectors of C at distance 0, 1, or 2 from (x, t).

Now consider a vector not in C: Let v be in $\mathbf{F}^{tn_i}$ and $f \in \mathbf{F}^l$, with $v \notin L$. Since $s = 1$, C has covering radius 1, so (v, f) is at distance 1 from C. It follows that for some $x \in L$ and some v_1 of weight 1 and length tn_i,

$$v = x + v_1. \tag{5.2}$$

Of course $v_1 = 0^{\alpha n_i} u 0^{\beta n_i}$ for some integers $\alpha, \beta \geq 0$ with $\alpha + \beta = t - 1$ and for some unit vector u of length n_i. Thus $(v; f)$ is at distance 1 from exactly t codewords, namely, $(x; f) + v_1 + v_2$, where v_2 is a unit vector congruent to v_1.

We now count the vectors of weight 2 in $\mathbf{F}^n$ that, added to $(v; f)$, produce a word in C. Of the three types of vectors of weight 2, namely, $(2; 0), (1; 1)$, and $(0; 2)$, indicating the weight on the first tn_i coordinates and on the last l, obviously there are none of the third type.

For type $(1; 1)$, there are exactly l of the form $(v_1; f_1)$, where f_1 is a unit vector of length l. But instead of v_1, we may choose any unit vector v_2 congruent to v_1, so there are exactly tl of type $(1; 1)$.

For type $(2; 0)$ we add $(v_3; 0^l)$ to $(x + v_1; f)$. On the left the result is $x + v_1 + v_3 \in L$. Since v_1 and v_3 have weights 1 and 2, resp., and since $v_1 + v_3 \in L$, $\mathrm{wt}(v_1 + v_3) \leq 3$ implies $\mathrm{wt}(v_1 + v_3) = 3$. By Lemma 5.1 *(iii)*, the number of vectors we seek of type $(2; 0)$ is

$$t^2(2^{i-1} - 1).$$

Therefore the number of vectors in C within distance 2 from a vector not in C is

$$N' := t + tl + t^2(2^{i-1} - 1). \tag{5.3}$$

Our code C is PMC iff $N = N'$. We will test a candidate code by seeing whether $N - N' = 0$. For future reference we record, without showing the routine algebra,

$$2(N - N') = (l - t)^2 + 2(l - t) + 2 - n. \tag{5.4}$$

16

5.1.3 Necessary and sufficient conditions for PMC

We now consider binary linear PMC (perfect multiple coverings) with radius 2. Let the linear $[n, k, d]$ code C be a perfect $(1/j, 1/j, 1/j)$-covering. Recall from [39] that this means that every vector in the space is within distance 2 of exactly j codewords. We now characterize all such codes C.

We first prove a necessary condition. Since (i) holds with no assumptions on s, we'll also use it in Section 5.2.

Theorem 5.1 *We use the previous notations.*

    (i)   *The length n of any binary linear PMC code C of radius 2 has the form $1 + \lambda^2$ for some integer λ.*

    (ii) *Moreover, when $s = 1$, we have*

$$2w = \lambda^2 - \lambda + 2 = t2^i$$
$$n - 2w = \lambda - 1 = l - t$$
$$l = t + \lambda - 1. \tag{5.5}$$

Proof. Since C is PMC, we see from Theorem 3.2 that its Lloyd polynomial $L(x)$,

$$jL(x) = 2x^2 - 2(n+1)x + 1 + n + \binom{n}{2}, \tag{5.6}$$

has w as a root. Solving (5.6) we find the roots are

$$\frac{1}{2}\left(n + 1 \pm \sqrt{n-1}\right). \tag{5.7}$$

It follows that $n = 1 + \lambda^2$ for some integer λ. If, as we may, we represent w with the negative sign in (5.7), we get (5.5). □

We now prove that the conditions of Theorem 5.1 are sufficient.

Theorem 5.2 *Let λ be any integer. Define $n := 1 + \lambda^2$, and let $i \geq 1$ and $t \geq 1$ be any integers satisfying*

$$\lambda^2 - \lambda + 2 = t2^i. \tag{5.8}$$

If $l := t + \lambda - 1$ is nonnegative, and setting $n' := t(2^i - 1) + l$, then define the binary linear $[n', i, t2^{i-1}]$ code $C^\perp$ as $S_i^t 0^l$, the t-fold repetition of S_i with l zeros appended. Then $C^\perp$ is a one-weight code; that weight is $w := t2^{i-1}$. Then $n' = n$, and C is an $[n, n-i]$ PMC code.

17

Proof. $n' = \lambda^2 - \lambda + 2 - t + l = \lambda^2 + 1 = n$. Since $l - t = \lambda - 1$, we find from (5.4) that

$$2(N - N') = (\lambda - 1)^2 + 2(\lambda - 1) + 2 - (1 + \lambda^2) = 0.$$

Therefore C is PMC, and $j = N = N'$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

The $[2, 1, 2]$ and $[2, 1, 1]$ codes are the only linear codes with $s = 1$ and $n = 2$; they are obviously PMC. The first of these is unique, as we show next.

Theorem 5.3 *The only binary linear PMC with radius 2 and $s = 1$ that has minimum distance 2 is the $[2, 1, 2]$ code.*

Proof. Under the previous notations $d = 2$ only if $l = 0$, and then $t(2^i - 1) = 1 + \lambda^2$. If $i \geq 2$ this equation has no integer solutions. For if p is a prime dividing $2^i - 1$, then -1 is a quadratic residue mod p, and hence $p \equiv 1 \pmod 4$. Applying this to every prime factor of $2^i - 1$ yields $2^i - 1 \equiv 1 \pmod 4$, a contradiction. Therefore $i = 1$ and C has to be an $[n, n-1, 2]$ code. We see that $n = 2$ by setting $l = 0$ in (5.5); we must take $\lambda = -1$. $\qquad\square$

We close this section with a short table of the PMC codes for $|\lambda| \leq 3$.

Table: PMC codes with $s = 1$ and $n \leq 10$

λ	n	$t2^i$	i	t	l	k	C	words
0	1	2	1	1	0	0	$[1, 0]$	0
1	2	2	1	1	1	1	$[2, 1, 1]$	$0*$
-1	2	4	1	2	0	1	$[2, 1, 2]$	a^2
2	5	4	1	2	3	4	$[5, 4, 1]$	$a^2 *^3$
			2	1	2	3	$[5, 3, 1]$	$a^3 *^2$
-2	5	8	1	4	1	4	$[5, 4, 1]$	$e_4 *$
			2	2	-1			
			3	1	-2			
3	10	8	1	4	6	9	$[10, 9, 1]$	$e_4 *^6$
			2	2	4	8	$[10, 8, 1]$	$p_6 *^4$
			3	1	3	7	$[10, 7, 1]$	$h_7 *^3$
-3	10	14	1	7	3	9	$[10, 9, 1]$	$e_7 *^3$

Key: $*^m$ is any element of $\mathbf{F}^m$; $a \in \mathbf{F}$; e_m is even-weight word in $\mathbf{F}^m$;
$p_6 \in <a^3 b^3, 100\,100, 010010>$; $h_7 \in [7, 4, 3]$ code.

5.2 The case $s = 2$

We have found the following *PMC* codes C in this case ($d = s = \delta = 2$):

C		$C^\perp$	
$[5, 1, 5]$	$j = 1$	$[5, 4; 2, 4]$	
$[5, 2, 2]$	$j = 2$	$[5, 3; 2, 4]$	
$[5, 3, 2]$	$j = 4$	$[5, 2; 2, 4]$	(5.9)
$[10, 7, 2]$	$j = 7$	$[10, 3; 4, 7]$	
$[37, 32, 2]$	$j = 22$	$[37, 5; 16, 22]$	
$[8282, 8269, 2]$	$j = 4187$	$[8282, 13; 4096, 4187]$	

The first is a classical perfect code. The notation $[n, k; w_1, w_2, \ldots]$ stands for an $[n, k]$ code in which all nonzero weights are among $w_1, w_2, \ldots$. In the above codes $C^\perp$ both weights are present, since $s = 2$. All the above codes C are *PMC* codes.

These codes arise from the following two constructions. We denote the i-dimensional simplex code by S_i, and the generator matrix of a code C by $g(C)$.

First Construction. We construct a 2-weight code $C^\perp$ by setting $g(C^\perp)$ equal to $g(S_i); c^h$ where c is any column of $g(S_i)$. For example, the $[5, 3, 2]$ code for $j = 4$ above has

$$g(C^\perp) = \begin{array}{|ccc|cc|} \hline 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ \hline \end{array}.$$

Here $i = 2$ and $h = 2$. There is no loss of generality in taking $c = (1, 0, 0, \ldots, 0)^T$.

In general we have

$$g(C^\perp) \;=\; g(S_i); c^h. \tag{5.10}$$

The weights in $C^\perp$ are 2^{i-1} and $2^{i-1} + h$.

We will now calculate the values

$$D := A_0(x), \; A_1(x), \; A_2(x)$$

for the cosets of C:

Identify the cosets with the syndromes, which are columns of S_i.

(i) The code C has

$$D = 1, 0, \binom{h+1}{2}$$

since column c occurs $h + 1$ times in $g(C^\perp)$.

(ii) For any column c' of $g(S_i)$ other than c,

$$D = 0, 1, \frac{2^i - 2}{2} + h,$$

since there are $(2^i - 2)/2$ vectors v of weight 2 in any coset of weight 1 in the Hamming code $S_i^\perp$. Column c is covered by one of those vectors v. We may replace c there by any of its h clones.

(iii) For column c,

$$D = 0, h + 1, \frac{2^i - 2}{2}.$$

Now the code C will be a PMC iff the sum of D is the same in all three cases:

$$j = 1 + \binom{h+1}{2} = 1 + h + \frac{2^i - 2}{2}. \tag{5.11}$$

This equation can be written

$$1 + \binom{h}{2} = 2^{i-1}. \tag{5.12}$$

All solutions of this Diophantine equation are known [38]. They exist precisely for $h = 0, 1, 2, 3, 6$, and 91.

Since h is the difference between the two weights in $C^\perp$, $h = \lambda$ as defined in Theorem 5.1. Thus we consider $h = \lambda = 0, 1, 2, 3, 6$, and 91. The corresponding values of j, from (5.11), are $j = 1, 2, 4, 7, 22, 4187$. Since $i = \dim(C^\perp)$, $i = n - k$. We may calculate i from (5.12). Because $s = 2$, we must have $i \geq 2$, which excludes the first two values of h. For the other four we get $n - k = 2, 3, 5, 13$, and we obtain the four largest codes in (5.9).

Second Construction. The $[5, 1, 5]$ code C has $s = R = 2$. Since it is perfect, it is a PMC with $j = 1$. If we now let C_2 be a coset of C of weight 2, and define $C_1 := C \cup C_2$, we get a $[5, 2, 2]$ code C_1. This construction obviously doubles the value of j for any PMC code with $R = 2$. Thus we get the second code in (5.9).

Since C_1 has $R = 2$ as well, we may arrive at the $[5, 3, 2]$ PMC code again by applying the second construction to C_1.

Remark 5.1 The first construction yields nothing if we repeat the simplex code in $C^\perp$. I.e., if $g(C^\perp) = t \times g(S_i); c^a$ then the smaller weight in $C^\perp$ is $t \cdot 2^{i-1} = 1 + \frac{\lambda^2 - \lambda}{2}$, from (5.7). The length is $n = t(2^i - 1) + \lambda = 1 + \lambda^2$, from Theorem 5.1. These easily imply $t = 1$.

Conjecture 5.1 *We conjecture the nonexistence of PMC codes with $d = s = \delta = 2$ other than those in (5.9).*

6 A Connection between weighted packings and coverings

From now on in this paper we assume that all the numbers m_i are non-negative.

It turns out that in this general set-up, the dual problems of finding all the best weighted packings and weighted coverings are really one and the same.

Suppose $M = (m_0, m_1, \ldots, m_\delta)$, and denote

$$v = \sum_{i=0}^{\delta} m_i \binom{n}{i} (q-1)^i,$$

If $v < 1$ then every code $C \subseteq \mathbf{F}_q^n$ is an M-packing and no C is an M-covering. The same is true also if $v = 1$ except that in that case the whole space is an M-covering. So, assume that $v > 1$ and $C \subset \mathbf{F}_q^n$, and denote $C' := \mathbf{F}_q^n \setminus C \neq \emptyset$. Then

$$<A(x), M> + <A'(x), M> = v$$

holds for all $x \in \mathbf{F}_q^n$, where $A'(x)$ is the weight distribution of C' with respect to x. Therefore, the condition

$$<A(x), M> \geq 1 \quad \text{for all} \quad x \in \mathbf{F}_q^n$$

is equivalent to the condition

$$<A'(x), M'> \leq 1,$$

where $M' = (m_0/(v-1), m_1/(v-1), \ldots, m_\delta/(v-1))$. Similarly, C is an M-packing if and only if C' is an M'-covering.

A similar observation is already true for multiple coverings and packings. If $M = (m_0, m_1, \ldots, m_\delta)$ and $m_i = 1/\mu$ for all $i = 0, 1, \ldots, \delta$, and we denote by $K_q(n, \delta, \mu)$ (resp. $A_q(n, \delta, \mu)$) the smallest (largest) possible number of codewords in any M-covering (M-packing) in $\mathbf{F}_q^n$ (again if $q = 2$ the subscript 2 is usually omitted), then

$$K_q(n, \delta, \mu) = q^n - A_q(n, \delta, V_q(n, \delta) - \mu),$$

where

$$V_q(n, \delta) = \sum_{i=0}^{\delta} \binom{n}{i} (q-1)^i.$$

21

Proposition 6.1 *Suppose $C \subseteq \mathbf{F}_q^n$ is an M-covering, where $M = (m_0, \ldots, m_\delta)$ and that $P \subseteq C$ is an M^*-packing, where $M^* = (m_0^*, \ldots, m_\delta^*)$, and let*

$$m = \max_{\sum m_i^* A_i \leq 1} \sum_{i=0}^{\delta} m_i A_i,$$

where maximum is taken over all A_i's. If $m < 1$, then the code $C \setminus P$ is an $(m_0/(1 - m), \ldots, m_\delta/(1 - m))$-covering.

Proof. Suppose $x \in \mathbf{F}_q^n$ and denote by $A_i^X(x) = |\{y \in X \mid d(y, x) = i\}|$. Then

$$\sum_{i=0}^{\delta} m_i A_i^C(x) \geq 1 \quad \text{and} \quad \sum_{i=0}^{\delta} m_i^* A_i^P(x) \leq 1$$

and hence

$$\begin{aligned}
\sum_{i=0}^{\delta} m_i A_i^{C \setminus P}(x) &\geq \sum_{i=0}^{\delta} m_i (A_i^C(x) - A_i^P(x)) \\
&\geq 1 - \sum_{i=0}^{\delta} m_i A_i^P(x) \geq 1 - m.
\end{aligned}$$

$\square$

Corollary 6.1 *Suppose C is an M-covering, where $M = (m_0, \ldots, m_\delta)$ and $P \subseteq C$ has minimum distance at least $2\delta + 1$. If*

$$m = \max_{0 \leq i \leq \delta} m_i < 1,$$

then $C \setminus P$ is an $(m_0/(1 - m), \ldots, m_\delta/(1 - m))$-covering.

$\square$

Corollary 6.2 $K(n, r, \mu) \leq K(n, r, \mu + 1) - A(n, 4r + 1)$.

Proof. See [25].

$\square$

7 Constructions of weighted coverings and packings

In this section we study only the binary case. All the weights are assumed to be non-negative. Some of the examples presented in this section were borrowed from [25] and [26].

7.1 Puncturing

Proposition 7.1 *If C is an $(m_0, m_1, \ldots, m_\delta)$-covering, then the punctured code C^* is an $(m_0^*, m_1^*, \ldots, m_{\delta-1}^*, m_\delta^*)$-covering where $m_i^* = \max\{m_i, m_{i+1}\}$ for $i = 0, 1, \ldots, \delta - 1$ and $m_\delta^* = m_\delta/2$, provided there are no two codewords in C that differ only in the punctured coordinate.*

Proof. Let $x \in \mathbf{F}^{n-1}$ be arbitrary. Denote by A_i^* the number of words of the punctured code C^* at distance i from x. If $\sum_{i=0}^{\delta-1} m_i^* A_i^*(x) \geq 1$ there is nothing to prove. Assume, therefore, that $\sum_{i=0}^{\delta-1} m_i^* A_i^*(x) < 1$. Then $\sum_{i=0}^{\delta-1} m_i A_i((x,0)) < 1$ and $\sum_{i=0}^{\delta-1} m_i A_i((x,1)) < 1$, and there are at least $\left(1 - \sum_{i=0}^{\delta-1} m_i^* A_i^*(x)\right) / m_\delta$ words y in C for which $d(y^*, x) = \delta$ and $d(y, (x,0)) = \delta$ and, similarly, there are at least $\left(1 - \sum_{i=0}^{\delta-1} m_i^* A_i^*(x)\right) / m_\delta$ words z in C such that $d(z^*, x) = \delta$ and $d(z, (x,1)) = \delta$, thus giving us $2\left(1 - \sum_{i=0}^{\delta-1} m_i^* A_i^*(x)\right) / m_\delta$ words u in C for which $d(u^*, x) = \delta$, proving our claim. $\square$

Corollary 7.1 *Suppose C is an M-covering of length n and radius r where $M = (1/\mu, \ldots, 1/\mu)$ and that no two codewords of C differ only in the first coordinate. Then there is an M'-covering of length $n - 1$ and radius r with the same number of codewords, where $M' = (1/\mu, 1/\mu, \ldots, 1/\mu, 1/(2\mu))$.* $\square$

Remark 7.1 We would like to point out the interesting fact that the sphere-covering lower bounds for $K(n, r, \mu)$ and the resulting weighted covering in the previous corollary are equal, and in that sense the resulting code is as good compared to the sphere-covering bound as the original one.

Example 7.1 The 192-element $(1,1)$-covering of length 11 defined in [17] has the property that no two codewords differ only in the first coordinate. Hence, by puncturing the first coordinate we obtain a $(1, 1/2)$-covering of length 10 with the same cardinality.

Proposition 7.2 *If P is an $(m_0, m_1, \ldots, m_\delta)$-packing, then P^* is a $(\min\{m_0, m_1\}, \min\{m_1, m_2\}, \ldots, \min\{\min_{\delta-1}, m_\delta\}, 0)$-packing.*

Proof. Let again $x \in \mathbf{F}^{n-1}$ be arbitrary. We use the same notation as in the previous proof. Denote further by $A_i'(x)$ the number of words $(p,1)$ in P for which $d(x, p) = i - 1$. Then

$$\sum_{i=0}^{\delta-1} A_i^*(x) \min\{m_i, m_{i+1}\} \leq \sum_{i=0}^{\delta-1} (A_i((x,0)) - A_i'((x,0)) + A_{i+1}'((x,0))) \min\{m_i, m_{i+1}\}$$

$$\leq \sum_{i=0}^{\delta-1} ((A_i((x,0)) - A_i'((x,0)))m_i + A_{i+1}'((x,0))m_{i+1})$$

$$= \sum_{i=0}^{\delta-1} A_i((x,0))m_i + A_\delta'((x,0))m_\delta \leq \sum_{i=0}^{\delta} A_i((x,0))m_i \leq 1.$$

$\square$

7.2 Shortening

If P is an $(m_0, \ldots, m_\delta)$-packing and we denote by P' the set of words c such that $(c, 0) \in P$, then it is easy to show that P is both an $(m_0, \ldots, m_\delta)$-packing and an $(m_1, m_2, \ldots, m_\delta)$-packing (by considering for each $x \in \mathbf{F}^{n-1}$ the densities at $(x,0)$ and $(x,1)$, respectively). If the sequence of weights is decreasing, then the latter statement is trivial.

7.3 Lengthening

Proposition 7.3 *Suppose C is an $(m_0, m_1, \ldots, m_\delta)$-covering. Adding a parity check bit to each word of C gives an $(m_0, \max\{m_0, m_1\}, \ldots, \max\{m_{\delta-1}, m_\delta\}, m_\delta)$-covering $\overline{C}$.*

Proof. Suppose $x \in \mathbf{F}^n$. Denote by $p(x) = wt(x) \pmod 2$. Then the weight distribution of $\overline{C}$ with respect to $(x, p(x))$ is $(A_0(x), 0, A_1(x) + A_2(x), 0, A_3(x) + A_4(x), \ldots, A_{\delta-1}(x) + A_\delta(x), 0)$ if δ is even and $(A_0(x), 0, A_1(x) + A_2(x), 0, A_3(x) + A_4(x), \ldots, A_{\delta-2}(x) + A_{\delta-1}(x), 0, A_\delta(x) + A_{\delta+1}(x))$ if δ is odd and the weight distribution of $\overline{C}$ with respect to $(x, 1 + p(x))$ is $(0, A_0(x) + A_1(x), \ldots, A_{\delta-1}(x) + A_\delta(x), 0)$ if δ is odd and $(0, A_0(x) + A_1(x), \ldots, A_{\delta-2}(x) + A_{\delta-1}(x), 0, A_\delta(x) + A_{\delta+1}(x))$ if δ is even. $\square$

It is sometimes possible to improve on the previous proposition.

Proposition 7.4 *[26] Suppose C is a $(1, 1, \ldots, 1, m_\delta = 1)$-covering of length n and covering radius δ, then the extended code $\overline{C}$ is a $(1, 1, \ldots, 1, m_{\delta+1} = 1/\lceil (n+1)/(\delta+1) \rceil)$-covering.*

Example 7.2 Adding a parity check bit to a 62-element $(1,1)$-covering of length 9 gives us a $(1, 1, 1/5)$-covering of length 10 with the same cardinality [26].

24

Proposition 7.5 *Suppose P is an $(m_0, m_1, \ldots, m_\delta)$-packing. Adding a parity check bit to each word of C gives an $(m_0, \min\{m_0, m_1\}, \ldots, \min\{m_{\delta-1}, m_\delta\})$-covering $\overline{C}$.*

Proof. The same as in the covering case. □

7.4 Direct sum

Proposition 7.6 *Suppose C is an $(m_0, m_1, \ldots, m_\delta)$-covering. Then the code $C \oplus \mathbf{F}$ is an $(m_0/2, \max\{m_0, m_1\}/2, \ldots, \max\{m_{\delta-2}, m_{\delta-1}\}/2, \max\{m_{\delta-1}/2, m_\delta\})$-covering (having radius δ) and an $(m_0/2, \max\{m_0, m_1\}/2, \ldots, \max\{m_{\delta-1}, m_\delta\}/2, m_\delta/2)$-covering (having radius $\delta + 1$).*

Proof. If $x \in \mathbf{F}^n$, then the weight distribution of both $(x, 0)$ and $(x, 1)$ with respect to $C \oplus \mathbf{F}$ equals $(A_0(x), A_0(x) + A_1(x), A_1(x) + A_2(x), A_2(x) + A_3(x), \ldots, A_{\delta-1}(x) + A_\delta(x), A_\delta(x) + A_{\delta+1}(x))$. □

Example 7.3 Applying the previous proposition to a 10-element $(1, 1/2)$-covering of length 5 obtained by the piecewise constant code construction in [26] we get a $(1/2, 1/2)$-covering of length 6 with 20 elements, which actually is the best known upper bound on $K(6, 1, 2)$ obtained by the matrix construction in [25].

Proposition 7.7 *Suppose P is an $(m_0, m_1, \ldots, m_\delta)$-packing. Then the code $C \oplus \mathbf{F}$ is an $(m_0/2, \min\{m_0, m_1\}/2, \ldots, \min\{m_{\delta-2}, m_{\delta-1}\}/2, \min\{m_{\delta-1}/2, m_\delta\})$-packing.* □

Proposition 7.8 *Suppose C' is an $(m'_0, m'_1, \ldots, m'_{\delta'})$-covering and C'' is an $(m''_0, m''_1, \ldots, m''_{\delta''})$-covering. Then their direct sum C is an $(m_0, m_1, \ldots, m_\delta)$-covering, where $\delta = \delta' + \delta''$ and $m_k = \max_{i+j=k} m'_i m''_j$.*

Proof. The result simply follows from the fact that

$$\sum_{i=0}^{\delta'} A'_i(x) m'_i \geq 1$$

and

$$\sum_{j=0}^{\delta''} A''_j(y) m''_j \geq 1$$

imply that

$$\left(\sum_{i=0}^{\delta'} A_i'(x) m_i' \right) \left(\sum_{j=0}^{\delta''} A_j''(y) m_j'' \right) \geq 1.$$

$\square$

We have no idea if the ADS construction [24] can be successfully generalized to the weighted covering case. Nevertheless, in the multiple covering case it is possible to generalize the concepts of normality and subnormality in a useful way [29]. For some applications of the ADS construction in the case of multiple coverings, see also [25].

7.5 $(u, u + v)$-construction

Proposition 7.9 *Suppose C' is an $(m_0', m_1', \ldots, m_{\delta'}')$-covering and C'' is an $(m_0'', m_1'', \ldots, m_{\delta''}'')$-covering. Then the code $\{(u, u + v) | u \in C', v \in C''\}$ is an $(m_0, m_1, \ldots, m_\delta)$-covering, where $\delta = \delta' + \delta''$ and $m_k = \max\limits_{i+j=k} m_i' m_j''$.* $\square$

Usually this construction is effective for codes with radius one. In the following proposition we denote $p(u) = wt(u) \pmod 2$.

Proposition 7.10 *Suppose $C \subset \mathbf{F}^n$ is an (m_0, m_1)-covering with $m_0 \leq 1$. Then the code $\{(p(u), u, u+c) | u \in \mathbf{F}^n, c \in C\}$ is an (m, m)-covering, where $m = m_1/(1+m_1-m_0)$, provided that $m_1 \leq m_0$, and it is an (m_0, m_1)-covering, provided that $m_1 > m_0$.*

Proof. It is easy to verify that the weight distribution of the resulting code with respect to a given word (x_0, x, y) is either $(A_0(x + y), A_1(x + y))$ or $(0, A_0(x + y) + A_1(x + y))$. $\square$

Example 7.4 Applying the previous construction to a perfect $(1/5, 1/5)$-covering consisting of all the 16 binary words of length 4, we obtain a perfect $(1/5, 1/5)$-covering of length 9 having 256 codewords, cf. [25].

Applying the previous construction to a $(1, 1/\mu)$-covering gives us a $(1, 1)$-covering (ordinary covering code), and we can always obtain at least as small a $(1, 1)$-covering by applying the construction to a $(1, 1)$-covering in the first place.

Proposition 7.11 *Suppose P is an (m_0, m_1)-packing. Then the code $\{(p(u), u, u + c) | u \in \mathbf{F}^n, c \in C\}$ is an (m, m)-packing, where $m = m_1/(1 + m_1 - m_0)$, provided that $m_1 \geq m_0$, and it is an (m_0, m_1)-packing if $m_1 < m_0$.* $\square$

7.6 Cascading

Sometimes it is useful to combine binary and nonbinary weighted coverings using a suitable variant of cascading that gives us a code whose length is the product of the lengths of the components.

Proposition 7.12 *Assume that $C_0 \subseteq \mathbf{F}^n$ satisfies the following two conditions:*

1. for all $x \in \mathbf{F}^n$ such that $d(x, C_0) \leq \sigma$ we have

$$\sum_{i=0}^{\delta} m_i^{(0)} A_i(x) \geq 1,$$

2. for all $x \in \mathbf{F}^n$ we have

$$\sum_{i=0}^{\delta} m_i^{(1)} A_i(x) \geq 1.$$

Assume further that $C_1, \ldots, C_{q-1}$ are disjoint translates of C_0 and that

$$C = C_0 \cup \cdots \cup C_{q-1}$$

has covering radius at most σ. Let $D \subseteq \mathbf{F}_q^N$ have covering radius at most R. Then the code

$$E = \bigcup_{(d_1, d_2, \ldots, d_N) \in D} C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_N}$$

has length nN, size $|D| \cdot |C_0|^N$ and is an $(m_0^*, m_1^*, \ldots, m_{N\delta}^*)$-covering, with

$$m_j^* = \max \; m_{j_1}^{(a_1)} m_{j_2}^{(a_2)} \ldots m_{j_N}^{(a_N)}$$

where the maximum is taken over all indices $j_1, \ldots, j_N$ such that $j_1 + \cdots + j_N = j$ and over all $a_1, \ldots, a_N$ such that $wt(a_1 \ldots a_N) \leq R$.

Proof. Let $x = (x_1, \ldots, x_N), x_i \in \mathbf{F}^n$, be arbitrary, and for each i choose $y_i \in \mathbf{F}_q$ such that $d(x_i, C_{y_i}) \leq \sigma$. Because D has covering radius at most R, there exists a word $d_1 d_2 \ldots d_N \in D$ whose distance to the word $y = y_1 \ldots y_N$ is at most R. Now consider the code $C_{d_1} \oplus \cdots \oplus C_{d_N}$. Denote by $A^{C_{d_j}}(x_j)$ the weight distribution of C_{d_j} with respect to x_j. Now we have

$$1 \leq \prod_{j=1}^{N} \left(\sum_{i=0}^{\delta} m_i^{(d(y_j, d_j))} A_i^{C_{d_j}}(x_j) \right)$$

$$\leq \sum_{t=0}^{N\delta} \left(\sum_{i_1 + \cdots i_N = t} \prod_{j=1}^{N} A_{i_j}^{C_{d_j}}(x_j) \cdot \max \; m_{i_1}^{(a_1)} m_{i_2}^{(a_2)} \ldots m_{i_N}^{(a_N)} \right)$$

$$\leq \sum_{t=0}^{N\delta} \left(\sum_{i_1 + \cdots i_N = t} \prod_{j=1}^{N} A_{i_j}^{C_{d_j}}(x_j) m_t^* \right)$$

where the maximum is taken over all indices $i_1, \ldots, i_N$ such that $i_1 + \cdots + i_N = t$ and over all $a_1, \ldots, a_N$ such that $wt(a_1 \ldots a_N) \leq R$. Our claim now follows because

$$A_t^E(x) \geq \sum_{i_1 + \cdots i_N = t} \prod_{j=1}^{N} A_{i_j}^{C_{d_j}}(x_j).$$

$\square$

In the previous construction we can choose a different system $C_0, \ldots, C_{q-1}, C$ for each of the N coordinates of D, and D can be a mixed code (its coordinates are over different alphabets).

7.7 Matrix construction

We now generalize the matrix construction [6]. Assume that $a^{(1)}, \ldots, a^{(N)} \in \mathbf{F}^n$ are (not necessarily distinct) column vectors whose linear span is the whole space $\mathbf{F}^n$ and that $S = \{s^{(1)}, \ldots, s^{(t)}\} \subseteq \mathbf{F}^n$. For every $k = 0, 1, \ldots, N$ and $y \in \mathbf{F}^n$, denote by $f_k(y)$ the number of different $(k+1)$-tuples $(i_1, \ldots, i_k, j)$ such that $i_1 < \ldots < i_k$ and

$$y = a^{(i_1)} + \ldots + a^{(i_k)} + s^{(j)}.$$

Proposition 7.13 *If*

$$\sum_{i=0}^{\delta} m_i f_i(y) \geq 1$$

for all $y \in \mathbf{F}^n$, then the code $\left\{(x_1, \ldots, x_N) \in \mathbf{F}^N | x_1 a_1 + \cdots + x_N a_N \in S\right\}$ is an $(m_0, m_1, \ldots, m_\delta)$-covering of cardinality $2^{N-n}t$.

Proof. For $z \in \mathbf{F}^N$, the number of words in the code that have distance exactly k to z equals the number of ways in which $y = Az$ can be represented as a sum

$$y = a^{(i_1)} + \cdots + a^{(i_k)} + s^{(j)},$$

for some $i_1 < \cdot < i_k$ and j, since the vector obtained by adding 1 to the coordinates $i_1, \ldots, i_k$ of z belongs to the code. In other words, this number equals $f_k(y)$. $\square$

Example 7.5 By choosing S and A as the set of the columns

$$
\begin{array}{ll}
01010 & 10001011 \\
01110 & 01000100 \\
00101 & 00100100 \\
01001 & 00011101
\end{array}
$$

we can check that each vector in $\mathbf{F}^4$ is in S or can be represented in at least three ways as a sum of an element in A and an element in S, hence the resulting 80-element code is a $(1, 1/3)$-covering of length 8 [26].

We have an analogous proposition for weighted packings.

Proposition 7.14 *If*

$$\sum_{i=0}^{\delta} m_i f_i(y) \leq 1$$

for all $y \in \mathbf{F}^n$, then the code $\left\{(x_1, \ldots, x_N) \in \mathbf{F}^N | x_1 a_1 + \cdots + x_N a_N \in S\right\}$ is an $(m_0, m_1, \ldots, m_\delta)$-packing of cardinality $2^{N-n} t$.

7.8 Piecewise constant codes

A piecewise constant code [17] of length $n = n_1 + n_2 + \cdots + n_i$ consists of all the words $(c_1, c_2, \ldots, c_i), c_i \in \mathbf{F}^{n_i}$, such that $(wt(c_1), wt(c_2), \ldots, wt(c_i)) \in W$, where W is a given subset of $\mathbf{Z}^i$. For such a code the weight distribution with respect to a given word $(x_1, x_2, \ldots, x_i)$ depends only on $(wt(x_1), wt(x_2), \ldots, wt(x_i))$, which essentially reduces the amount of checking.

Example 7.6 As mentioned in [26] the words of weights 0, 2, 5 and 7 in $\mathbf{F}^7$ form a $(1, 1/3)$-covering. In fact, the density of this covering is equal to 1 at all except the 14 points that have weight 1 or 6, at which the density is 7/3. In the same way we can check, for instance, that the words of weights 2 and 5 form a $(1/6, 1/6, 1/12)$-covering and the density of this covering is equal to 1 at all points except the all-zero and the all-one points, at which it is 21/12.

8 Acknowledgements

References

[1] E. F. Assmus, Jr., and H. F. Mattson, Jr., "Error-correcting codes: an axiomatic approach," *Information and Control* 6, 1963, pp. 315–330.

[2] E. F. Assmus, Jr., H. F. Mattson, Jr., and R. Turyn, "Cyclic codes," Final Report, Contract no. AF 19(604)–8516, AFCRL, April 28, 1966. Sylvania Applied Research Laboratory, Waltham, Mass. (Document no. AFCRL–66–348.)

[3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory,* Bibliographisches Institut, Mannheim - Wien - Zürich, 1985.

[4] V. M. Blinovsky, "List decoding," *Discr. Math.* 106/107, 1992, pp. 45–51.

[5] B. Bouchon, and G. Cohen, "Partitions and Fuzziness," *J. of Math. Analysis and Applications* 116, no. 1, 1986, pp. 166–183.

[6] A. Blokhuis and C. W. H. Lam. "More coverings by rook domains," *J. Comb. Theory A* 36, 1984, pp. 240–244.

[7] L. A. Bassalygo, G. V. Zaitsev, and V. A. Zinoviev, "On Uniformly Packed Codes," *Problems of Inform. Transmission* 10, no. 1, 1974, pp. 9–14.

[8] L. A. Bassalygo and V. A. Zinoviev, "Note on Uniformly Packed Codes," *Problems of Inform. Transmission,* vol. 13, no. 3, 1977, pp. 22–25.

[9] A. R. Calderbank, and P. Delsarte, "On error-correcting codes and invariant linear forms," *SIAM J. Discr. Math.* 6, no. 1, 1993, pp. 1–23.

[10] W. Chen and D. Li, "Lower bounds for multiple covering codes," in preparation.

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

[12] G. D. Cohen, P. Frankl, "On tilings of the binary vector space," *Discrete Math.,* 31, 1980, pp. 271–277.

[13] G. D. Cohen, I. S. Honkala, and S. N. Litsyn, "On weighted coverings and packings with diameter one," in book: *EUROCODE'92,* ICMS, No.339, Springer-Verlag, pp.43–49, 1993.

[14] 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, pp. 328–343.

[15] G. D. Cohen, S. N. Litsyn, and H. F. Mattson, Jr., "On perfect weighted coverings with small radius," *Springer Lecture Notes in Computer Science*, 573, 1992, pp. 32–41.

[16] G. D. Cohen, S. N. Litsyn, and H. F. Mattson, Jr., "Binary perfect weighted coverings, I, the linear case," *Sequences II*, Capocelli, DeSantis, Vaccaro, Eds., Springer-Verlag, 1993, pp. 36–51.

[17] 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, pp. 680–694.

[18] P. Delsarte, "Four fundamental parameters of a code and their combinatorial significance," *Information and Control* 23, 1973, pp. 407–438.

[19] P. Elias, "Error-correcting codes for list decoding," *IEEE Trans. Inform. Theory* 37, 1991, pp. 5-12.

[20] T. Etzion and G. Greenberg, "Constructions for Perfect Mixed Codes and Other Covering Codes," *IEEE Trans. Inform. Theory* 39, 1993, pp. 209–214.

[21] J. M. Goethals, and S. L. Snover, "Nearly Perfect Binary Codes," *Discrete Math.* 3, 1972, pp. 65–88.

[22] J. M. Goethals, and H. C. A. van Tilborg, "Uniformly packed codes," *Philips Res. Repts* 30, 1975, pp. 9–36.

[23] M. J. E. Golay, Binary coding, IEEE PGIT (*Trans. Inform. Theory*) 4, 1954, pp. 23–28.

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

[25] H. O. Hämäläinen, I. S. Honkala, M. K. Kaikkonen, and S. N. Litsyn, "Bounds for multiple covering codes," *Designs, Codes and Cryptography* 3, 1993, pp. 251–275.

[26] H. O. Hämäläinen, I. S. Honkala, S. N. Litsyn and P. R. J. Östergård, "Bounds for binary codes that are multiple coverings of the farthest-off points," *SIAM J. Discr. Math.*, to appear.

[27] H. O. Hämäläinen, I. S. Honkala, S. N. Litsyn, and P. R. J. Östergård, "Football pools - a game for mathematicians," *American Mathematical Monthly*, to appear.

[28] H. O. Hämäläinen and S. Rankinen, "Upper bounds for football pool problems and mixed covering codes," *J. Comb. Theory A* 56, 1991, pp. 84-95.

[29] I. S. Honkala, "On the normality of multiple covering codes," *Discrete Math.* 125, 1994, pp. 229-239.

[30] M. Karpovsky, "Weight distribution of translates, covering radius and perfect codes correcting errors of the given multiplicities," *IEEE Trans. Inform. Theory* 27, 1981, pp. 462–472.

[31] D. Li and W. Chen, "New lower bounds for binary covering codes," *IEEE Trans. Inform. Theory* 40, 1994, pp. 1122–1129.

[32] J. H. van Lint, "Recent results on covering problems," *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: Proceedings of the 6th International Conference AAECC-6*, Rome, Italy, July 1988 (T. Mora, Ed.), Springer-Verlag, Berlin, pp. 7–21.

[33] J. H. van Lint, Jr., "Covering radius problems," Master's thesis, Eindhoven University of Technology, 1988.

[34] S. P. Lloyd, Binary block coding, *Bell Syst. Tech. J* 36, 1957, pp. 517–535.

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

[36] P. R. J. Östergård, "New upper bounds for the football pool problem for 11 and 12 matches," *Journal of Comb. Theory A*, vol.67, No. 2, 1994, pp.161–168.

[37] N. V. Semakov, V. A. Zinoviev, G. V. Zaitsev, "Uniformly Packed Codes," *Problems of Inform. Transmission* 7, 1971, no. 1, pp. 38–50.

[38] Th. Skolem, P. Chowla, and D. J. Lewis, "The Diophantine equation $2^{n-2} - 7 = x^2$ and related problems," *Proc. Amer. Math. Soc.* 10 , 1959, pp. 663–669.

[39] 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, no. 3, 1991, pp. 678–682.

[40] Z. Zhang, "Linear inequalities for covering codes: Part I—Pair covering inequalities," *IEEE Trans. Inform. Theory* 37, 1991, pp. 573–582.

[41] Z. Zhang and C. Lo, "Linear inequalities for covering codes: Part II—Triple covering inequalities," *IEEE Trans. Inform. Theory* 38, 1992, pp. 1648–1662.