9-1991

Binary Perfect Weighted Coverings (PWC) I. The Linear Case

G. D. Cohen

S. N. Litsyn

H. F. Mattson Jr

SU-CIS-91-34

Binary Perfect Weighted Coverings (PWC)
I. The Linear Case

G. D. Cohen, S. N. Litsyn, and H.F. Mattson, Jr.

September 1991

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

BINARY PERFECT WEIGHTED COVERINGS (PWC)[1]

I. The Linear Case

Gérard D. Cohen
Ecole Nationale Supérieure des Télécommunications
46 rue Barrault, C-220-5
75634 Paris cédex 13, France
Email: Cohen@inf.enst.fr

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

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

[1]This paper was presented by invitation at SEQUENCES '91, Methods in Communication, Security, and Computer Science, Positano, Italy, June 17–21, 1991. It will appear in the Proceedings, to be published by Springer in the LNCS series.

Abstract

This paper deals with an extension of perfect codes to fractional (or weighted) coverings. We shall derive a Lloyd theorem—a strong necessary condition of existence—and start a classification of these perfect coverings according to their diameter. We illustrate by pointing to list decoding.

1 Introduction

Most codes involved in error-correction use nearest-neighbor decoding, i.e., the output of the decoder is the nearest codeword to the received vector. There has been renewed interest lately (see, e.g., [11]) in list decoding, where the decoder output is a list with given maximal size: correct decoding now means that the actually transmitted codeword is in the list. The size of the list could be constant (see the perfect multiple coverings studied in [17]) or an increasing function of the distance between the received vector and the code, so as to guarantee a given level of confidence. For example, a codeword would be given a list consisting of itself ($m_0 = 1$ in our notations), whereas vectors at distance R (the covering radius of the code) would have lists of maximal size. An application of list codes could be to spelling checking, with the code being the English vocabulary, and the "ambient" space being any combination of letters with maximal length n.

2 Notations and known special cases

We denote by $\boldsymbol{F}^n$ the vector space of binary n-tuples, by $d(\cdot\ ,\ \cdot)$ the Hamming distance, by $C[n,k,d]R$ a linear code C with length n, dimension k, minimum distance $d = d(C)$ and covering radius R [8]. In this paper we consider only codes with $d \geq 2$. We denote the Hamming weight of $x \in \boldsymbol{F}^n$ by $|x|$.

$A(x) = (A_0(x), A_1(x) \ldots A_n(x))$ will stand for the weight-distribution of the coset $C + x, x \in \boldsymbol{F}^n$; thus

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

Given an $(n+1)$-tuple $M = (m_0, m_1, \ldots, m_n)$ of weights, i.e., rational numbers in $[0,1]$, 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 consider only *coverings*, i.e., codes C such that $\theta(x) \geq 1$ for all x.

(2.2) C is a *perfect M-covering* if $\theta(x) = 1$ for all x.

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

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

To avoid trivial cases, we usually assume that $m_i = 0$ for $i \geq n/2$, i.e., $\delta < n/2$.

Here are the known special cases.

(2.3) Classical perfect code: $m_i = 1$ for $i = 0, 1, \ldots \delta$.

(2.4) Perfect multiple coverings: $m_i = 1/j$ for $i = 0, 1, \ldots \delta$
where j is a positive integer [17, 6].

(2.5) Perfect L-codes: $m_i = 1$ for $i \in L \subseteq \{1, 2, \ldots \lfloor n/2 \rfloor\}$. See [13] and [7].

3 The covering equality

For a perfect M-covering C one gets from the definition:

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

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

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

For $i = 0$, the second sum is $|C| = 2^k$, for $i = 1$ it is $2^k n$, and so on. Hence we get the following analog of the Hamming condition.

Proposition 3.1 A covering C is a perfect M-covering if and only if

(3.1) $$\sum_{i=0}^{n} m_i \binom{n}{i} = 2^{n-k}$$

□

As mentioned earlier, we want to avoid trivial solutions to (3.1) as, e.g.,

$$\begin{aligned} m_i &= 1 \quad \text{for all } i \ (k=0), \\ m_i &= 1 \quad \text{for } 0 \le i \le \lfloor n/2 \rfloor \text{ for odd } n \ (k=1). \end{aligned}$$

In fact, we are interested in getting perfect M-coverings with small diameter. However, we shall prove in the next section a strong lower bound on δ.

We can interpret (3.1) in a geometrical way: we define a weighted sphere around any vector c in $\boldsymbol{F}^n$ by means of the function

$$\mu_c(x) := m_{d(c,x)}. \tag{3.2}$$

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

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

then (3.1) becomes

$$\mu(S(c,\delta)) = 2^{n-k}$$

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

Equation (3.2) is reminiscent of a *fuzzy membership* function, as studied, e.g., in [5].

4 A Lloyd theorem

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

$$P_{n,i}(x) = \sum_{0 \le j \le i} (-1)^j \binom{n-x}{i-j} \binom{x}{j}. \tag{4.1}$$

We now prove

Theorem 4.1 *An $[n,k,d]$ R code C is a perfect $(m_0, m_1, \ldots, m_\delta)$-covering only if the Lloyd polynomial*

$$L(x) := \sum_{0 \le i \le \delta} m_i \, P_i(x)$$

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

Corollary 4.1 $s \leq \delta$.

Proof of the Theorem: (Adapted from [1], Chapter II, Section 1, which records A. M. Gleason's proof of the classical Lloyd theorem.) We use the group algebra $\mathcal{A}$ of all formal polynomials

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

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

Define

(4.2) $$S := \sum_{0 \leq i \leq \delta} m_i \sum_{|a|=i} X^a.$$

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

(4.3) $$C := \sum_{c \in C} X^c.$$

Then we find from Section 3 that

(4.4) $$SC = \sum_{c \in C} X^c \cdot S \; = \; \boldsymbol{F}^n := \sum_{a \in \boldsymbol{F}^n} X^a.$$

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

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

We use linearity to extend χ_u to a linear functional defined on $\mathcal{A}$:
For all $Y \in \mathcal{A}$ if $Y = \sum_{a \in \boldsymbol{F}^n} \gamma_a X^a$, then $\chi_u(Y) := \sum \gamma_a \chi_u(a)$.
It follows that

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

It is known [1, 10] that for any $u \in \boldsymbol{F}^n$, if $|u| = w$, then

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

It follows that

$$\chi_u(S) \; = \; L(w).$$

From (4.4), furthermore, we see that

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

for all $u \neq 0$.

Now if $u \in C^{\perp}$, then

$$\chi_u(C) \;=\; \sum_{c \in C} (-1)^{u \cdot c} \;=\; |C| \;=\; 2^k.$$

Thus $\chi_u(S) = 0$. □

5 The case when $\delta = s$

By a result of Delsarte [10], (3.10), one can always choose $\delta = s$. Let us reformulate his result.

Proposition 5.1 *A code C is a perfect M-covering with $\delta(M) = s$. In that case the m_i's are uniquely determined by*

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

where α_i is the i^{th} coefficient in the Krawtchouk expansion of the annihilator polynomial $\alpha(x)$ of $C^{\perp}$. 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 $C^{\perp}$.

5.1 Uniformly packed codes

In [2] a code is called *uniformly packed* (u.p.) if there exist rational numbers $\alpha_0, \alpha_1, \ldots \alpha_R$ such that for any x in $\boldsymbol{F}^n$, $\sum \alpha_i A_i(x) = 1$ holds. An extensive account of u.p. codes appears in [12]. With our notations, this reads:

Proposition 5.2 *A uniformly packed code C is a perfect M-covering with $\delta(M) = R(C)$.*

In that case, $R = s = \delta$ and Proposition 5.1 applies. The reason is that $R \leq s \leq \delta$ in general. The first inequality is Delsarte's Theorem, (3.3) of [10]; the second is Corollary 4.1.

Examples of u.p. codes (see [10], Section (3.1)):

$$\begin{aligned} QR[47, 24, 11]7, &\quad \text{with } M = (1, 1, 1, 1, 1/9, 1/9, 1/9, 1/9) \\ \text{extended } QR[48, 24, 12]8, &\quad \text{with } M = (1, 1, 1, 1, 5/27, 1/9, 1/9, 1/9, 1/54). \end{aligned}$$

5.2 Strongly uniformly packed codes

This concept is introduced in [15]: An $[n, k, d = 2e+1]R$ code C is *strongly uniformly packed* (s.u.p.) if $R \leq e+1$ and for any x such that $d(x, C) \geq e$, the following holds:

$$|B(x, e+1) \cap C| \;=\; r \text{ (independent of } x).$$

Here $B(x, e+1)$ denotes the sphere of radius $e+1$ centered at x in $\boldsymbol{F}^n$. Of course, if $d(x, C) \leq e-1$, then by the triangle inequality

$$|B(x, e+1) \cap C| \;=\; 1.$$

Such a code will be denoted by $SUP(n, e, r)$. We have just proved

Proposition 5.3 *An $SUP(n, e, r)$ is a perfect M-covering with $m_0 = m_1 = \cdots = m_{e-1} = 1, m_e = m_{e+1} = 1/r$.* □

Note that a code C can be a perfect M-covering for different M's. For example, the $[23, 12, 7]3$ Golay code is an $SUP(23, 3, 6)$, hence a perfect $(1, 1, 1, 1/6, 1/6)$-covering by Proposition 5.3. On the other hand, since this code is perfect, it is also a perfect $(1, 1, 1, 1)$-covering. We saw in (5.1) a sufficient condition for the uniqueness of M.

5.3 The case of diameter one

If $\delta = 1$, then $R = s = 1$, and $L(x) = m_0 + m_1(n - 2x) = -2xm_1 + 2^{n-k}$. Theorem (4.1) implies that $C^\perp$ has a unique nonzero weight, namely, $x = 2^{n-k-1}/m_1$.

Since $d \geq 2$, $C^\perp$ has no coordinates identically 0. Therefore $C^\perp$ consists of $1/m_1$ copies of the simplex code [14] with $m_1 = 1/t$, for some integer t. Thus $n = t(2^{n-k}-1)$.

Now from $m_0 + m_1 n = 2^{n-k}$, we get $m_0 = 2^{n-k} - n/t = 1$ (which also follows directly from $d \geq 2$).

Proposition 5.4 *A perfect M covering with $\delta = 1$ exists iff $n = t(2^i - 1)$, $m_0 = 1$, $m_i = 1/t$ for some integer t.*

Proof. The "only if" part is proved just above. The "if part" also! Namely, take for C the dual of the code consisting of t copies of the simplex code. □

For its intrinsic interest we shall present an alternate description of these $\{1, 1/t\}$-coverings.

Definitions. Let $C[n,k,d]R$ and $C'[n',k',d']R'$ be two linear codes.

$$\text{Set } \chi_c(x) = \begin{cases} 0 & \text{if } x \in C \\ 1 & \text{otherwise.} \end{cases}$$

Note that χ_c is the complement of the usual indicator function. We then extend this function to a mapping $X : \boldsymbol{F}^{nn'} \to \boldsymbol{F}^{n'}$ by setting

$$\chi(x) := (\chi_c(x_1),\ \chi_c(x_2), \ldots \chi_c(x_{n'}))$$

where the x_i's are in $\boldsymbol{F}^n$, for $1 \leq i \leq n'$, and

$$x = (x_1, x_2, \ldots x_{n'}) \text{ is their concatenation.}$$

We are now ready to define $C \otimes C'$ as follows:

$$C \otimes C' := \left\{ z \in \boldsymbol{F}^{nn'} : \chi(z) \in C' \right\}.$$

Remark that $C \otimes C'$ is *not linear* in general, because χ_c is not.

Proposition 5.5 *$C \otimes C'$ has length nn', minimum distance $\min\{d, d'\}$, and covering radius RR'.*

Proof. Easy. □

Proposition 5.6 *Suppose that $d(C') \geq 2$. Then $C \otimes C'$ is linear if and only if C is an $[n, n-1]$ code. In that case, $C \otimes C'$ is an $[nn', nn' - (n' - k')]$ code.*

Proof. If C is an $[n, n-1]$ code, then χ_c is linear (check!), and so is χ, and $C \otimes C' = \chi^{-1}(C')$.

Conversely, suppose C has codimension at least 2. Let a, b be in different cosets of C; then $\chi_c(a) = \chi_c(b) = \chi_c(a+b) = 1$. Let c' be a word of C' with first component $= 1$ and $x = (a, x_2, x_3, \ldots, x_{n'})$ a codeword of $C \otimes C'$(i.e., in $\chi^{-1}(C')$). Then $y := (b, x_2, x_3 \ldots, x_{n'})$ is also in $\chi^{-1}(C')$. Now $x + y = (a + b, 0, 0 \ldots, 0)$ is not in $C \otimes C'$, since $\chi(x + y) = (1, 0, \ldots 0) \notin C'$. Hence $C \otimes C'$ is not linear.

Let us now prove the dimensional part of the proposition: consider χ', the restriction of χ to $C \otimes C'$. Since $ker\ \chi \subset C \otimes C'$, $ker\ \chi' = ker\ \chi$. But $\dim(ker\ \chi) = n' \cdot \dim C = n'(n-1)$. Combined with $Im(\chi') = C'$, this yields:

$$\begin{aligned} \dim C \otimes C' &= \dim(Im(\chi')) + \dim(ker(\chi')) \\ &= k' + n'(n-1) \\ &= nn' - (n' - k'). \end{aligned}$$

□

To avoid $d(C) = 1$, and hence $d(C \otimes C') = 1$, we choose for C the parity code $[n, n-1, 2]1$ which is unique with such parameters. Then $C \otimes C'$ is an $[nn', nn' - (n' - k'), 2]R'$ code.

Proposition 5.7 *Let x and x' be such that $d(x, C) = R, d(x', C') = R'$. Suppose that $A_R(x)$ and $A'_{R'}(x')$ are independent of x. Then for $C \otimes C'$ the coefficient $A_{RR'}(z)$ is the same for any z such that $d(z, C \otimes C') = RR'$, and*

$$A_{RR'} \;=\; A_R \; A'_{R'}.$$

□

Corollary 5.1 *The "if" part of Proposition 5.4 (alternate proof).*

$$\begin{array}{lll} \textit{Choose} & C[t, t-1, 2]1 & A_1 = t \\ & C'[2^i - 1, 2^i - i - 1, 3]1 & A'_1 = 1 \end{array}$$

Then $C \otimes C'$ is a $[t(2^i - 1), t(2^i - 1) - i, 2]1$ with $A_1(x) = t$ for all $x \notin C \otimes C'$, i.e., a $\{1, 1/t\}$-covering. □

If we omit the condition $m_0 = 1$, i.e., we set $d = 1$, we get an extended family of PWC by adding to all code words from PWC in Corollary 5.1 all possible tails of length l. Let C be $[t(2^i - 1),\ t(2^i - 1) - i, 2]1$ PWC, and C'' consist of all vectors (c, x) of length $t(2^i - 1) + l$, where c belongs to C, and x is from F^l.

Proposition 5.8 *C'' is a $[t(2^i - 1) + l, t(2^i - 1) + l - i, 1]1$ PWC, i.e., a $\{1 - l/t, 1/t\}$-covering.*

Proof. Linearity and parameters are trivial. Let us consider a vector $y = (y_1, y_2)$, where y_1 and y_2 are from $F^{t(2^i-1)}$ and F^l respectively. If y_1 belongs to C, then $A_0(y) = 1$ and $A_1(y) = l$ (all the code vectors of the shape (y_1, x), $d(y_2, x) = 1$). If $d(y_1, C) = 1$, then $A_0(y) = 0$, and $A_1(y) = t$ (all the code words of shape (z, y_2), $d(z, y_1) = 1$). Solving the system $m_0 + l \cdot m_1 = 1,\ t \cdot m_1 = 1$, we get the statement.

From the uniqueness of the above system we conclude

Proposition 5.9 *For $\delta = 1$ all the possible PWC are described in Proposition 5.8.*

Remark. In particular, setting $l = t - 1$ in Proposition 5.8 gives a complete characterization of the parameters of binary linear PMC with diameter 1, simpler than the one in [15].

6 The case of diameter 2

Now we take $\delta = 2$. By Corollary 4.1, we know that s is at most 2. We shall treat separately the two possible values of s. First, notice the obvious implication following from (2.1):

$$m_0 \neq 1 \Longrightarrow d \leq \delta.$$

Under the assumption $\delta = 2$ this becomes

$$m_0 \neq 1 \Longrightarrow d \leq 2. \tag{6.1}$$

Therefore, if the code C corrects at least one error, then $m_0 = 1$. Since $R \leq s \leq 2$, C is quasi-perfect and, in fact, (λ, μ) uniformly packed. Much is known, although not everything, about these codes [12, 10], and we shall not consider them here. Hence we assume

$$m_0 \neq 1, \quad \text{which implies} \quad d = 2$$

from (6.1) and our blanket assumption $d \geq 2$. In fact, we shall restrict ourselves to perfect multiple coverings (2.2); i.e., set

$$m_0 = m_1 = m_2 = 1/j.$$

From the definition in Theorem 4.1, the Lloyd polynomial $L(x)$ satisfies

$$jL(x) = 2x^2 - 2(n+1)x + 1 + n + \binom{n}{2}. \tag{6.2}$$

If we use (3.1) we may write

$$jL(x) = 2x^2 - 2(n+1)x + j2^{n-k}. \tag{6.3}$$

Since $s \geq 1$, $L(x)$ has at least one integral root. But the sum of the roots is $n+1$, so both are integral. Solving (6.1) we find that the roots of $L(x)$ are

$$\frac{1}{2}\left(n + 1 \pm \sqrt{n-1}\right) = 1 + \frac{m^2 \pm m}{2}, \tag{6.4}$$

where we have set

$$n = 1 + m^2 \tag{6.5}$$

for some integer m.

6.1 PMC with $s = 1$

Proposition 6.1 *The only perfect multiple covering code with $s = 1$, $d = 2$, and $\delta = 2$ is the $[2, 1, 2]$ code with $j = 2$.*

Proof. Let C be an $[n, k, d]$ code satisfying the hypotheses. Since $d = 2$, $C^\perp$ has repeated coordinates but none identically zero. Therefore $C^\perp$ is, for some integer $t \geq 2$, the t-fold repetition of the simplex code [14] of type $[2^i - 1, i, 2^{i-1}]$, where $i = \dim\ C^\perp = n - k$. Thus $n = t(2^{n-k} - 1)$. From (6.5) we get

$$t(2^{n-k} - 1) = 1 + m^2. \tag{6.6}$$

But there are no solutions for (6.6) if $n - k \geq 2$. For let p be any prime dividing $2^{n-k} - 1$. Then -1 is a quadratic residue mod p, from (6.6). Therefore $p \equiv 1 \pmod 4$. It follows that $2^{n-k} - 1 \equiv 1 \pmod 4$, a contradiction.

Therefore there are no PMC with $\delta = 2$ and $s = 1$ except for $n - k = 1$. And in this case there is only the $[2, 1, 2]$ code. The reason is that with $d \geq 2$ it must be the $[n, n-1, 2]$ code. From the definition in Section 1 it easily follows that n can be only 2. □

Allowing d to be 1, we find that the only possibility for the check matrix is the t-fold repetion of $g(S_i)$ (generator matrix of a simplex code of length $2^i - 1$) with l zero-columns appended, yielding $n = t(2^i - 1) + l$. It amounts to appending all possible tails of length l to codewords described in Corollary 5.1. It is easy to check that there are 2 kinds of covering equalities (namely, vectors coinciding with, or being at distance 1 from, codewords on the first $t(2^i - 1)$ coordinates):

$$\begin{aligned} m_0 + lm_i \ &+ \ \tbinom{t}{2}(2^i - 1)m_2 + \tbinom{l}{2}m_2 = 1 \\ tm_1 \ &+ \ (2^{i-1} - 1)\, t^2 m_2 + tlm_2 = 1. \end{aligned}$$

This implies

$$t^2 - t(2^i + 1 + 2l) + (l^2 + l + 2) = 0$$

which has discriminant

$$D = (2^i + 1)^2 + 2^{i+2}l - 8.$$

We get a PMC iff $D = x^2$ has integer solutions. For example, the values $i = 3, l = 3, t = 14$ yield the PMC $[101, 98]$ with $j = 644$. Of course, for $i = t$ we get $8l + 1 = x^2$ having all odd x as solutions.

Parameters of a series of PMC for $s = 1, \delta = 2$:

$$i = 1 \quad l = \tfrac{x^2-1}{8}, \qquad x \equiv \pm 1 \pmod 4;$$

$$i = 2 \quad l = \tfrac{x^2-1}{16} - 1, \quad x \equiv \pm 1 \pmod 8;$$

$$i = 3 \quad l = \tfrac{x^2-3}{32} - 2, \quad x \equiv \pm 3 \pmod{16};$$

$$i = 4 \quad l = \tfrac{x^2-25}{64} - 4, \quad x \equiv \pm 5 \pmod{32};$$

$$i = 5 \quad l = \tfrac{x^2-57}{128} - 8, \quad x \equiv \pm 21 \pmod{64};$$

Conjecture 6.1 *For every i there exists an infinite series of PMC iff $(2^i - 7)$ is a square mod 2^{i+1}.*

Derivation of parameters $[n, k, 1]$

$$t_{1,2} = (2^i + 2 + l \pm x)/2;\ n = t(2^i - 1) + l;\ j = (2^{i-1} - 1)t^2 + t(1 + l);\ k = n - i;$$

If the above conjecture is true (checked for i up to 10), then

Theorem 6.1 *(based on Conjecture 6.1) Let $a = \pm\sqrt{2_{i+1} - 7} \pmod{2^{i+2}}$. Then for $x \equiv a \pmod{2^{i+1}}$ there is a PMC code with parameters*

$$l = \tfrac{x^2 - 2^{i+1} + 7}{2^{i+2}} - 2^{i-2},$$

$$t = (2^i + 2 + l \pm x)/2;$$

$$n = t(2^i - 1) + l;$$

$$k = n - i;$$

$$j = (2^{i-1} - 1)t^2 + t(1 + l).$$

6.2 PMC with $s = 2$

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

(6.7)

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

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 $C^\perp$, since $s=2$, both weights are present. All the above codes C are PMC codes.

These codes arise from the following two constructions.

Notation

$g(C)$	generator matrix of code C
S_i	i-dimensional simplex code

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

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

Here $i=2$ and $h=2$. There is no loss of generality in taking c to be a unit vector.

In general we have

(6.8) $$g(C^\perp) \;=\; g(S_i);c^h.$$

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:

$$j \;=\; 1 + \binom{h+1}{2} \;=\; 1 + h + \frac{2^i - 2}{2}\,. \tag{6.9}$$

This equation can be written

$$1 + \binom{h}{2} \;=\; 2^{i-1}. \tag{6.10}$$

All solutions of this Diophantine equation are known [16]. They exist precisely for $h = 0, 1, 2, 3, 6,$ and 91.

Since h is the difference between the two weights in $C^{\perp}$, $h = m$ as defined in (6.4) and (6.5). Thus we consider

$$h = m = 0, 1, 2, 3, 6, \text{ and } 91.$$

The corresponding values of j, from (6.9), are

$$j = 1, 2, 4, 7, 22, 4187.$$

Since $i = \dim(C^{\perp})$, $i = n - k$. We may calculate i from (6.10). We get

$$n - k = 0, 1, 2, 3, 5, 13.$$

The first two cases have $s = 0$ and 1. They are nevertheless the PMC codes C shown here:

C	j	$C^{\perp}$
$[1, 1; 1]$	1	$[1, 0; 0]$
$[2, 1; 2]$	2	$[2, 1; 2]$.

The next cases are the $[5,3,2]$ code in our table (6.7), and the three larger codes of (6.7).

It remains to account for the $[5,1;5]$ code and the $[5,2,2]$ code.

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 (6.7).

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.

Note. The first construction yields nothing if we repeat the simplex code in $C^\perp$. I.e., if

$$g(C^\perp) \ = \ t \times g(S_i); c^m$$

then the smaller weight in $C^\perp$ is

$$t \cdot 2^{i-1} \ = \ 1 \ + \ \frac{m^2 - m}{2},$$

from (6.4). The length is

$$n \ = \ t(2^i - 1) \ + \ m \ = \ 1 \ + \ m^2,$$

from (6.5). These easily imply $t = 1$. We have proved

Proposition 6.2 *The only PMC codes with $d = s = \delta = 2$ obtainable by the First Construction are those in (6.7).*

Conjecture 6.2 *We conjecture the nonexistence of PMC codes with $d = s = \delta = 2$ other than those in (6.7).*

7 List codes

Recall from the introduction that in list decoding, to every x in F^n (received vector) is attached a list of at most K candidates (transmitted codewords). Following [4, 11], we denote by (n, e, K) a code C enabling the correction of up to e errors by list decoding with maximal list size K. This is equivalent to

$$|B(x,e) \cap C| \leq K \ \text{ for all } \ x, \tag{7.1}$$

where $B(x, e)$ denotes the sphere of radius e centered at x. A code satisfying (7.1) is also called a K-fold e-packing, and a perfect multiple covering (2.2) if equality holds in (7.1) for all x (see [17]). From (5.2), the following is immediate.

Proposition 7.1 *An* $SUP(n, e, r)$ *is a list code* $(n, e+1, r)$.

Refining the definition of a list code, we denote by $\mathcal{K} = \{K_i\}$ the set of possible list sizes attached to x's, with $\max K_i = K$. Here is a small table of these codes.

n	e	$\mathcal{K}$	Comments
23	4	$\{1, 6\}$	Golay code
23	5	$\{1, 22\}$	Golay code
47	7	$\{1, 9\}$	QR
48	8	$\{1, 24, 29, 34, 39, 44, 45, 49, 54\}$	Ext. QR

Acknowledgement

We are pleased to acknowledge that this problem arose in discussions with I. Honkala in Veldhoven in June, 1990.

References

[1] E. F. Assmus, Jr., H. F. Mattson, Jr., 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.)

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

[3] L. A. Bassalygo, G. V. Zaitsev, V. A. Zinoviev, "note On uniformly Packed Codes," *Problems of Inform. Transmission*, vol. 13, no. 3, 1977, pp. 22–25.

[4] V. M. Blinovskii, "Bounds for codes in the case of list decoding of finite volume," *Problems Inform. Transmission* 22, no. 1, (1986), pp. 7–19 (English).

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

[6] R. F. Clayton, "Multiple Packings and Coverings in Algebraic Coding Theory," Thesis, Univ. of California, Los Angeles, 1987.

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

[8] G. D. Cohen, M. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, "Covering radius—Survey and recent results," *IEEE Trans. Inform. Theory* **IT-31**, pp. 328–343, 1985.

[9] A. A. Davydov, L. M. Tombak, "Number of minimal-weight words in block codes," *Problems of Inform. Transmission*, vol. 24, no. 1, pp. 11–24, 1988.

[10] P. Delsarte, "Four Fundamental Parameters of a Code and Their Combinatorial Significance," *Information and Control*, vol. 23, no. 5, pp. 407–438, 1973.

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

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

[13] M. Karpovsky, "Weight Distribution of Translates, covering radius and perfect codes correcting errors of the given multiplicities," *IEEE Trans. Inform. Theory* IT-27, pp. 462–472, 1981.

[14] J. E. MacDonald, "Design methods for maximum minimum-distance error-correcting codes," *IBM J. Res. Devel.* vol. 4, pp. 43–57, 1960.

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

[16] 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.

[17] G. J. M. van Wee, G. D. Cohen, S. N. Litsyn, "A note on Perfect Multiple Coverings of Hamming Spaces," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 678–682, May 1991.