Journal of Integer Sequences, Vol. 9 (2006),
Article 06.4.7

The Number of Inequivalent $(2R+3,7)R$ Optimal Covering Codes

Gerzson Kéri[1]
Computer and Automation Research Institute
Hungarian Academy of Sciences
Kende u. 13–17
H-1111 Budapest
Hungary
keri@sztaki.hu

Patric R. J. Östergård[2]
Department of Electrical and Communications Engineering
Helsinki University of Technology
P.O. Box 3000
02015 TKK
Finland
patric.ostergard@tkk.fi

Abstract

Let $(n, M)R$ denote any binary code with length n, cardinality M and covering radius R. The classification of $(2R+3, 7)R$ codes is settled for any $R = 1, 2, \dots$, and a characterization of these (optimal) codes is obtained. It is shown that, for $R = 1, 2, \dots$, the numbers of inequivalent $(2R+3, 7)R$ codes form the sequence $1, 3, 8, 17, 33, \dots$ identified as A002625 in the *Encyclopedia of Integer Sequences* and given by the coefficients in the expansion of $1/((1-x)^3(1-x^2)^2(1-x^3))$.

1 Introduction

Let $(n, M)R$ denote a binary code of length n, cardinality M and covering radius R. Throughout the paper, unless otherwise mentioned, we assume that R is an arbitrary pos-

[1]Supported in part by the Hungarian National Research Fund, OTKA, Grant No. T043276.
[2]Supported in part by the Academy of Finland, Grants No. 107493 and 110196.

itive integer. We assume familiarity with basic concepts of coding theory; the Hamming weight of a word x is denoted by $\mathrm{wt}(x)$ and the Hamming distance between two words x, y is denoted by $d(x, y)$. For an introduction to coding theory in general and covering codes in particular, see [9] and [3], respectively.

We shall here focus on $(2R+3, 7)R$ codes, that is, 7-word binary codes in the Hamming space Z_2^{2R+3} with covering radius R. Cohen et al. [4] proved that $(2R+3, 7)R$ codes exist and that $(2R+3, 6)R$ codes do not exist. Denoting the minimum number of codewords in any binary code C of length n and covering radius R by $K(n, R)$, this means that $K(2R+3, R) = 7$ for all $R \geq 1$.

Our goal is to settle the classification of $(2R+3, 7)R$ codes and characterize the optimal codes for any $R \geq 1$, thereby providing a solution to [5, Research Problem 7.31]. Two binary codes are *equivalent* if one can be obtained from the other by a permutation of the coordinates followed by a transposition of the coordinate values in some of the coordinates. It will be shown that, for $R = 1, 2, \ldots$, the number of equivalence classes of $(2R+3, 7)R$ codes coincides with the coefficients of x^{R-1} in the expansion of

$$\frac{1}{(1-x)^3(1-x^2)^2(1-x^3)}.$$

This integer sequence, starting with $1, 3, 8, 17, 33, 58, 97, 153, 233, \ldots$, is sequence A002625 in the *Encyclopedia of Integer Sequences*.

2 Some Old Results with an Extension

We first review some partial results for the classification of $(2R+3, 7)R$ codes. In fact, very few classification results are known for optimal binary covering codes in general; the following list [5, Sect. 7.2.6] summarizes the sets of parameters that have been settled: (a) $M < 7$ and arbitrary n; (b) $M = 7$ and $1 \leq R \leq 3$; and (c) the six sporadic cases $K(6, 1) = 12$, $K(7, 1) = 16$, $K(8, 1) = 32$, $K(8, 2) = 12$, $K(9, 2) = 16$ and $K(23, 3) = 4096$.

The optimal $(5, 7)1$, $(7, 7)2$ and $(9, 7)3$ codes have been classified by Stanton and Kalbfleisch [11]; Östergård and Weakley [10] (with misprinted codes; the codes are reproduced in correct form by Bertolo, Östergård and Weakley [2]); and Kaski and Östergård [5], respectively. The main result of the current paper relies on the classifications of $(5, 7)1$ and $(7, 7)2$ codes; the numbers of such codes are 1 and 3, respectively.

We shall now describe the structure of the $(5, 7)1$ and $(7, 7)2$ codes. For this purpose we consider the following $(1, 7)0$ codes C_i (the codewords are labelled, so we present the codes as tuples rather than multisets of words):

$$
\begin{array}{rcl}
C_1 & = & (0,0,0,1,1,1,1), \\
C_2 & = & (0,0,1,0,1,1,1), \\
C_3 & = & (0,1,0,0,1,1,1), \\
C_4 & = & (0,1,1,1,0,0,1), \\
C_5 & = & (0,1,1,1,0,1,0), \\
C_6 & = & (0,1,1,1,1,0,0).
\end{array} \tag{1}
$$

Using the notation $|.|.|$ for coordinate-wise concatenation of codes or words, the optimal $(5,7)1$ and $(7,7)2$ codes can be described as follows, up to equivalence.

Theorem 2.1. *(a) The unique* $(5,7)1$ *code is* $C = |C_1|C_2|C_3|C_4|C_5|$.
(b) The three $(7,7)2$ *codes are* $|C|C_1|C_1|$, $|C|C_4|C_4|$ *and* $|C|C_6|C_6|$.

An inspection of the equivalence classes of the three $(7,7)2$ codes gives a result that is needed later.

Corollary 2.1. All $(7,7)2$ *codes of the form* $|C_1|C_2|C_3|C_4|C_5|D|$ *that contain the all-zero word are obtained by letting* $D = |C_i|C_j|$ *with* $i = j$ *or* $i = 6$ *or* $j = 6$.

The codes discussed so far may also be presented using the following alternative notation, which disregards the order of the coordinates. Let $C(n_1, n_2, n_3, n_4, n_5, n_6)$ denote the code that is the concatenation of C_1 taken n_1 times, C_2 taken n_2 times, and so on. Note that different presentations may lead to equivalent codes. The automorphism group of $|C_1|C_2|C_3|C_4|C_5|C_6|$ is generated by the following permutations of coordinates: (1 2), (1 2 3), (4 5), (4 5 6) and (1 4)(2 5)(3 6). These permutations acting on the indices n_i of $C(n_1, n_2, n_3, n_4, n_5, n_6)$ then give equivalent codes. This observation will be used later in the proof of Theorem 3.3.

For example, the codes in Theorem 2.1 can be presented as

$$
\begin{array}{rcl}
C & \equiv & C(1,1,1,1,1,0), \\
|C|C_1|C_1| & \equiv & C(3,1,1,1,1,0), \\
|C|C_4|C_4| & \equiv & C(1,1,1,3,1,0), \\
|C|C_6|C_6| & \equiv & C(1,1,1,1,1,2).
\end{array}
$$

Observe that for these codes exactly five of the values of n_i are odd, and their covering radius is $(\sum_{i=1}^{6} n_i - 3)/2$. In fact, these examples are covered by the following general result.

Theorem 2.2. *Let* $n = \sum_{i=1}^{6} n_i$ *be an odd integer where* $n_1, n_2, n_3, n_4, n_5, n_6$ *are non-negative integers. Then, the covering radius of* $C(n_1, n_2, n_3, n_4, n_5, n_6)$ *is* $(n-3)/2$ *if and only if exactly one of* $n_1, n_2, n_3, n_4, n_5, n_6$ *is even.*

Proof. Let us assume first that exactly one of the n_is is even. Then, it can be assumed that n_1, n_2, n_3, n_4, n_5 are odd and n_6 is even, by symmetry. Let $x = |x_1|x_2|x_3|x_4|x_5|x_6|$ be any word in the binary Hamming space Z_2^n where $x_i \in Z_2^{n_i}$ and x is partitioned according to the structure of $C(n_1, n_2, n_3, n_4, n_5, n_6)$, the ith codeword of which we denote by c_i. Let w_i be the weight of x_i. Then we have

$$\begin{aligned}
d(x, c_1) &= w_1 + w_2 + w_3 + w_4 + w_5 + w_6,\\
d(x, c_2) &= w_1 + w_2 + (n_3 - w_3) + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6),\\
d(x, c_3) &= w_1 + (n_2 - w_2) + w_3 + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6),\\
d(x, c_4) &= (n_1 - w_1) + w_2 + w_3 + (n_4 - w_4) + (n_5 - w_5) + (n_6 - w_6),\\
d(x, c_5) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + w_4 + w_5 + (n_6 - w_6),\\
d(x, c_6) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + w_4 + (n_5 - w_5) + w_6,\\
d(x, c_7) &= (n_1 - w_1) + (n_2 - w_2) + (n_3 - w_3) + (n_4 - w_4) + w_5 + w_6,
\end{aligned}$$

and consequently

$$d(x, C) \leq \frac{2d(x, c_1) + \sum_{i=2}^{7} d(x, c_i)}{8} = \frac{4\sum_{i=1}^{6} n_i}{8} = n/2. \tag{2}$$

Assume that $d(x, C) > (n-3)/2$. Then $d(x, C) = (n-1)/2$ (since n is odd and $d(x, C) \leq n/2$). As $\mathrm{wt}(c_1)$, $\mathrm{wt}(c_6)$, $\mathrm{wt}(c_7)$ have the same parity and $\mathrm{wt}(c_2)$, $\mathrm{wt}(c_3)$, $\mathrm{wt}(c_4)$, $\mathrm{wt}(c_5)$ have the same parity—this can be seen by looking at the parities of n_i—consequently also $d(x, c_1)$, $d(x, c_6)$, $d(x, c_7)$ have the same parity and $d(x, c_2)$, $d(x, c_3)$, $d(x, c_4)$, $d(x, c_5)$ have the same parity. The sum of the eight distances $d(x, c_1)$ (taken twice), $d(x, c_2)$, $d(x, c_3)$, $\ldots$, $d(x, c_7)$ is $4n$, cf. (2), and each of these is at least $(n-1)/2$, so we get that exactly four of these must be $(n-1)/2$ and the other four must be $(n+1)/2$, from which it follows that $d(x, c_1) = d(x, c_6) = d(x, c_7)$ and $d(x, c_2) = d(x, c_3) = d(x, c_4) = d(x, c_5)$. Then

$$\begin{aligned}
3n &= d(x, c_1) + 2d(x, c_4) + d(x, c_5) + d(x, c_6) + d(x, c_7)\\
&= 5n_1 - 4w_1 + 3n_2 + 3n_3 + 3n_4 + 3n_5 + 3n_6\\
&= 3n + (2n_1 - 4w_1),
\end{aligned}$$

so $2n_1 - 4w_1 = 0$ and thereby $w_1 = n_1/2$, which is not possible since n_1 is odd.

If $w_i = \lceil \frac{n_i}{2} \rceil$ for $i = 1, 2, \ldots, 6$, then $d(x, C) = (n-3)/2$, so the covering radius is exactly $(n-3)/2$.

To prove the sufficiency, suppose that the number of even n_is is greater than 1, that is, 3 or 5. We may assume that either n_1, n_2, n_3; or n_1, n_2, n_4; or n_1, n_2, n_3, n_4, n_5 are even and the remaining n_is are odd, again by symmetry. In all cases, let $w_i = \lfloor \frac{n_i}{2} \rfloor$ for $i = 1, 2, 3, 5$ and $w_i = \lceil \frac{n_i}{2} \rceil$ for $i = 4, 6$, where w_i is again the weight of x_i in a partitioned word $x = |x_1|x_2|x_3|x_4|x_5|x_6|$. For each case, we obtain $d(x, C) \geq (n-1)/2$, so the covering radius of C cannot be $(n-3)/2$. □

3 Classification and Characterization

We prove in this section that any $(2R + 3, 7)R$ code is equivalent to a code that belongs to the family examined in Theorem 2.2 by the help of a classification result regarding surjective codes.

Definition 1. *A binary code C is called 2-surjective if each of the four pairs of bits* (00, 01, 10 *and* 11) *occurs in at least one codeword, for any pair of coordinates.*

It is known [6, 8] that no 2-surjective M-word code exists of length

$$n > \binom{M-1}{\lfloor (M-2)/2 \rfloor}.$$

For $M = 7$ this means that no 2-surjective code exists if $n > 15$. As regards the case when $M = 7$ and $5 \leq n \leq 15$, a classification of all such 2-surjective codes has been carried out [7]. It turns out [7, Table 1] that the only $(2R + 3, 7)R$ code that is 2-surjective is the unique $(5, 7)1$ code.

Theorem 3.1. *For $R \geq 2$, there are no 2-surjective $(2R + 3, 7)R$ codes.*

We are now prepared to prove the main theorem of this paper.

Theorem 3.2. *If $C^{(R)}$ is a $(2R + 3, 7)R$ code where $R \geq 2$, then*

$$C^{(R)} \equiv C(n_1, n_2, n_3, n_4, n_5, n_6) \tag{3}$$

where exactly one of $n_1, n_2, n_3, n_4, n_5, n_6$ is even.

Proof. The code $C^{(R)}$ is not 2-surjective according to Theorem 3.1, and consequently $C^{(R)} \equiv |C^{(R-1)}|X|$ where $C^{(R-1)}$ is of length $2R + 1$ and X is of length 2 with a nonzero covering radius. As the covering radius of a partitioned code cannot be less than the sum of the covering radii of its parts, the covering radius of $C^{(R-1)}$ has to be $R - 1$ (it cannot be $R - 2$ [7, Theorem 7]) and the covering radius of X has to be 1. By a repeated application of this argument we obtain that

$$C^{(R)} \equiv |C^{(1)}|X^{(1)}|X^{(2)}| \cdots |X^{(R-1)}| \tag{4}$$

where $C^{(1)}$ is of length 5 and covering radius 1 and each $X^{(i)}$ is of length 2 and covering radius 1. Then the covering radius of $|C^{(1)}|X^{(i)}|$ has to be 2 for $i = 1, 2, \ldots, R - 1$ (since the order of the parts $X^{(i)}$ is arbitrary), so by Theorem 2.1,

$$C^{(1)} \equiv |C_1|C_2|C_3|C_4|C_5| = C, \tag{5}$$

and then

$$C^{(R)} \equiv |C|Y^{(1)}|Y^{(2)}| \cdots |Y^{(R-1)}|, \tag{6}$$

where $|C|Y^{(i)}|$ is a $(7, 7)2$ code for all i and (having transposed coordinate values, if necessary) $|C|Y^{(1)}|Y^{(2)}| \cdots |Y^{(R-1)}|$ contains the all-zero word. But then Corollary 2.1 tells that all $Y^{(i)}$ have the form $|C_j|C_k|$ and so $C^{(R)} \equiv C(n_1, n_2, n_3, n_4, n_5, n_6)$ for some values of n_i. By Theorem 2.2, such a code has covering radius $(n - 3)/2$ if and only if exactly one of $n_1, n_2, n_3, n_4, n_5, n_6$ is even. □

By [7, Theorem 7], Theorem 3.2 characterizes all optimal binary covering codes of size 7.

Theorem 3.3. *For any positive integer R, the number $Q(R)$ of inequivalent $(2R+3,7)R$ codes is equal to*

(a) the number of different integer solutions of the system

$$\begin{aligned} &m_1+m_2+m_3+m_4+m_5+m_6=R-1,\\ &m_1\ge m_2\ge m_3\ge 0,\\ &m_4\ge m_5\ge 0,\\ &m_6\ge 0; \end{aligned} \tag{7}$$

(b) the coefficient of x^{R-1} in the expansion

$$\sum_{R=1}^{\infty} Q(R)x^{R-1} = \frac{1}{(1-x)^3(1-x^2)^2(1-x^3)}. \tag{8}$$

Proof. (a) By Theorems 2.2 and 3.2, a code is a $(2R+3,7)R$ code if and only if it is equivalent to a code of form

$$C(2m_1+1, 2m_2+1, 2m_3+1, 2m_4+1, 2m_5+1, 2m_6), \tag{9}$$

where $m_1, m_2, m_3, m_4, m_5, m_6$ are non-negative integers and $\sum_{i=1}^{6} m_i = R-1$. By the discussion in Section 2 it follows that a code like this is equivalent to another code of similar form $C(2m'_1+1, 2m'_2+1, 2m'_3+1, 2m'_4+1, 2m'_5+1, 2m'_6)$ if and only if $\{m_1, m_2, m_3\} = \{m'_1, m'_2, m'_3\}$, $\{m_4, m_5\} = \{m'_4, m'_5\}$ and $m_6 = m'_6$ (using set notation for multisets).

(b) If we originate $Q(R)$ from (a), then clearly

$$Q(R) = \sum_{\substack{N_1+N_2+N_3=R-1\\ N_1,N_2,N_3\ge 0}} P(N_1,1)P(N_2,2)P(N_3,3), \tag{10}$$

where $P(N,t)$ denotes the number of different partitions of N with at most t positive parts, for which it is well known [1] that

$$\sum_{N=0}^{\infty} P(N,t)x^N = \prod_{j=1}^{t} \frac{1}{1-x^j}. \tag{11}$$

This completes the proof, because (10) and (11) imply (8). □

Finally, observe that the full automorphism group of (9) is of order $AB(2m_1+1)!(2m_2+1)!\cdots(2m_6)!$, where

$$A = \begin{cases} 6, & \text{if } m_1=m_2=m_3;\\ 2, & \text{if } m_1=m_2\ne m_3 \text{ or } m_1=m_3\ne m_2 \text{ or } m_2=m_3\ne m_1;\\ 1, & \text{otherwise;} \end{cases}$$

$$B = \begin{cases} 2, & \text{if } m_4=m_5;\\ 1, & \text{otherwise.} \end{cases}$$

Acknowledgments

The authors thank a referee for useful comments and for pointing out incomplete argumentation in the original manuscript.

References

[1] G. E. Andrews, *The Theory of Partitions*, Addison-Wesley, Reading, 1976.

[2] R. Bertolo, P. R. J. Östergård and W. D. Weakley, An updated table of binary/ternary mixed covering codes, *J. Combin. Des.* **12** (2004), 157–176.

[3] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, Elsevier, Amsterdam, 1997.

[4] 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.

[5] P. Kaski and P. R. J. Östergård, *Classification Algorithms for Codes and Designs*, Springer, Berlin, 2006.

[6] G. O. H. Katona, Two applications (for search theory and truth functions) of Sperner type theorems, *Period. Math. Hungar.* **3** (1973), 19–26.

[7] G. Kéri and P. R. J. Östergård, Further results on the covering radius of small codes, *Discrete Math.*, accepted for publication.

[8] D. J. Kleitman and J. Spencer, Families of k-independent sets, *Discrete Math.* **6** (1973), 255–262.

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

[10] P. R. J. Östergård and W. D. Weakley, Classification of binary covering codes, *J. Combin. Des.* **8** (2000), 391–401.

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

2000 *Mathematics Subject Classification*: Primary 94B75; Secondary 05B40, 94B25.
Keywords: covering radius, classification of codes, integer sequence.

(Concerned with sequences A001399, A001400, A001401, A002625, and A072921.)

Received January 11 2006; revised version received September 22 2006 Published in *Journal of Integer Sequences*, September 22 2006.

Return to Journal of Integer Sequences home page.