Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 43 (2002), No. 2, 445-449.

Classifying Optimal Ternary Codes of Length 5 and Covering Radius 1

Patric R. J. Östergård* **William D. Weakley**

Department of Computer Science and Engineering
Helsinki University of Technology
P.O. Box 5400, 02015 HUT, Finland
e-mail: patric.ostergard@hut.fi

Department of Mathematical Sciences
Indiana University – Purdue University Fort Wayne
Fort Wayne, Indiana 46805
e-mail: weakley@ipfw.edu

Abstract. It is well known that optimal ternary codes of length 5 and covering radius 1 have 27 codewords. The structure of such optimal codes has been studied, but a classification of these is still lacking. In this work, a complete classification is carried out by constructing codes coordinate by coordinate in a backtrack search. Linear inequalities and equivalence checking are used to prune the search. In total there are 17 optimal codes.

Keywords: backtrack search, code equivalence, covering code, football pool problem, nonlinear code, ternary code

1. Introduction

Let Z_q^n denote the set of all n-tuples $(x_1, \ldots, x_n)$ with $x_i \in Z_q = \{0, \ldots, q-1\}$. The covering radius of a code $C \subseteq Z_q^n$ is the smallest R such that all words in Z_q^n are within Hamming distance R from at least one codeword in C. A q-ary code with length n, covering radius R, and cardinality M is called an $(n, M)_q R$ code. A central problem in combinatorial coding

*Supported by the Academy of Finland.

theory is that of determining $K_q(n, R)$, which denotes the smallest M such that an $(n, M)_qR$ code exists. An $(n, K_q(n, R))_qR$ code is called *optimal*. See [2] for an extensive survey of covering codes.

The problem of determining $K_3(n, 1)$ is known as the *football pool problem*. In the 1960s, Kamps and Van Lint [3] proved that $K_3(5, 1) = 27$. The tricky part of this proof is the lower bound, as the upper bound $K_3(5, 1) \leq 27$ is obtained directly by lengthening the $(4, 9)_31$ Hamming code.

Knowing that $K_3(5, 1) = 27$, one may proceed further and classify $(5, 27)_31$ codes up to equivalence; two codes in Z_q^n are *equivalent* if one can be obtained from the other by a permutation of the coordinates and permutations of the coordinate values, one for each coordinate. Kolev [4] studied $(5, 27)_31$ codes and proved that all such codes have at least one coordinate with the property that the three subcodes obtained by deleting this coordinate are equivalent to the $(4, 9)_31$ Hamming code. As in [7], we say that such a code is *split* in this coordinate. In [7], it is shown that although in a sense every optimal $(8, 32)_21$ code C can be obtained from two subcodes equivalent to the $(7, 16)_21$ Hamming code, not every C is split.

In Section 2, we discuss methods for classifying covering codes. These can essentially be divided into methods that complete the code word by word, and ones that go coordinate by coordinate. In this work, we use the latter approach. We prune the search by using linear inequalities, given below, and also by detecting equivalent subcodes. Our classification reveals 17 optimal $(5, 27)_31$ codes and is verified by obtaining the same codes with an alternative approach that assumes the result by Kolev [4] on the structure of such codes. A complete list of the codes is given in Section 3, including a discussion of some of their properties.

2. Classifying covering codes

An $(n, M)_qR$ code can be expressed using an $n \times M$ matrix with entries from Z_q. As with any other incidence structure, backtrack search may be used to build up such matrices, either column by column (codeword by codeword) or row by row (coordinate by coordinate). Both of these approaches have been used for covering codes earlier in, for example, [7] and [6], respectively.

There are two basic ways of pruning this backtrack search. First, we may use the fact that the final code must have covering radius R. Second, it is only necessary to consider one (sub)code from each equivalence class.

In this work we carry out equivalence tests on all subcodes. We transform the codes to be tested into graphs and use the graph automorphism program *nauty* [5]. Such a transformation is presented for binary codes in [7], to which the interested reader is referred for details; a generalization to q-ary codes is straightforward.

In constructing a code word by word, the covering property can be utilized in the search by picking an uncovered word and requiring that it be covered by the next word chosen [7]. In proceeding coordinate by coordinate, on the other hand, we have a set of linear inequalities that must be fulfilled.

The following approach was first used in [3, 8] together with combinatorial arguments. It is used in [1, 6] to obtain new bounds for binary covering codes.

For given lengths m and n with $m \leq n$ and a given word $x \in Z_3^m$, let $Q_x \subseteq Z_3^n$ denote the set of 3^{n-m} words whose first m coordinates coincide with x. Moreover, given a code C of length n and covering radius 1, let $M_x = |Q_x \cap C|$, and let $B(x) = \{y \in Z_3^m \mid d(x,y) = 1\}$. Since all words in Q_x must be covered by a codeword, we have that

$$(2n - 2m + 1)M_x + \sum_{y \in B(x)} M_y \geq 3^{n-m}, \; x \in Z_3^m. \tag{1}$$

We have the additional equalities

$$M_{z0} + M_{z1} + M_{z2} = M_z. \tag{2}$$

For $m = 1, 2, \ldots$, we now solve (using any software of choice) the integer linear programming instances given by (1), (2), and if we have a solution for $m = n$, then there exists an $(n, M)_3 1$ code. Moreover, a complete classification can be carried out by finding all such solutions and accepting only one code from each equivalence class.

In the intermediate stages we also require that

$$M_x \leq 3^{n-m}, \tag{3}$$

since no codeword occurs more than once in an optimal code.

By applying this method, we obtained the following results for $(5, 27)_3 1$ codes. The number of inequivalent subcodes fulfilling (1), (2), (3) for $1 \leq m \leq 5$ is 7, 40, 148, 22, and 17. So there are 17 inequivalent $(5, 27)_3 1$ codes.

We verified this result using an alternative approach. Assuming the result by Kolev [4], one may construct a $(5, 27)_3 1$ code as $C = \{s0, t1, u2 : s \in C', t \in C'', u \in C'''\}$, where C', C'', and C''' are equivalent to the unique optimal $(4, 9)_3 1$ Hamming code H. Since $|\mathrm{Aut}(H)| = 432$, the number of distinct codes equivalent to H is

$$\frac{n!(q!)^n}{|Aut(H)|} = \frac{4!6^4}{432} = 72.$$

We may fix C' and choose C'' and C''' among the 72 distinct codes; here repetitions are allowed, and order does not matter. We checked these $73 \cdot 72/2 = 2628$ combinations and found 17 inequivalent codes, which coincide with the codes found earlier.

3. The codes

Before describing the classified codes, we define a set of invariants, also used in [7], that is useful in distinguishing the codes. Given words v, w in Z_q^n, let $D(v, w)$ be the set of indices of coordinates where v and w differ. Clearly the cardinality of $D(v, w)$ is the Hamming distance $d(v, w)$ between v and w.

Let C be a code in Z_q^n and d a positive integer. For some non-negative integer k, there will be k distinct sets $D_1, \ldots, D_k$ that occur as sets $D(v, w)$ as we examine pairs v, w of words of C satisfying $d(v, w) = d$. For each i, $1 \leq i \leq k$, let m_i denote the number of occurrences of D_i; we may assume that the D_i's are ordered so that $m_i \geq m_{i+1}$ for each i, $1 \leq i < k$.

Then let $S_d(C)$ denote the ordered k-tuple $[m_1, \ldots, m_k]$. It is easily seen that if C_a and C_b are equivalent codes, then $S_d(C_a) = S_d(C_b)$ for each d.

In the list of codes below, we give for each code C_i enough of the values $S_d(C_i)$ to distinguish C_i from the other codes, except that $S_d(C_{13}) = S_d(C_{14})$ for all d. These two codes may be distinguished in other ways. For example, $S_1(C_{13}) = S_1(C_{14}) = [3]$, but in C_{13} the three adjacencies involve only three words (a triangle is formed), while in C_{14} six words are involved (there are three independent edges).

We will take the Hamming code H in Z_3^4 to be all linear combinations of 1102 and 1202 over Z_3. By [4], for any $(5, 27)_3 1$ code C, there are $\tau_1, \tau_2 \in \mathrm{Aut}(Z_3^4)$ such that $C = \{s0, t1, u2 : s \in H, t \in \tau_1(H), u \in \tau_2(H)\}$. For our purpose, it suffices to use automorphisms that permute the values in each coordinate. We describe these as follows. The six permutations of Z_3 will be labeled π_1 = identity, $\pi_2 = (0,1,2)$, $\pi_3 = (0,2,1)$, $\pi_4 = (1,2)$, $\pi_5 = (0,2)$, and $\pi_6 = (0,1)$, where each permutation is given in cycle form. Then let $\pi[m_1, m_2, m_3, m_4]$ denote the automorphism of Z_3^4 that applies the permutation π_{m_i} in the ith coordinate.

C_1: $\tau_1 = \tau_2$ = identity. $S_1(C_1) = [27]$ and $|\mathrm{Aut}(C_1)| = 2592$. This is just 3 copies of H, and $\mathrm{Aut}(C_1) \cong \mathrm{Aut}(H) \times S_3$.

C_2: τ_1 = identity, $\tau_2 = \pi[1,4,5,6]$. $S_1(C_2) = [15]$ and $|\mathrm{Aut}(C_2)| = 72$.

C_3: τ_1 = identity, $\tau_2 = \pi[1,1,3,2]$. $S_1(C_3) = [9]$, $S_2(C_3) = [18]$, and $|\mathrm{Aut}(C_3)| = 108$.

C_4: τ_1 = identity, $\tau_2 = \pi[1,4,5,2]$. $S_1(C_4) = [11]$ and $|\mathrm{Aut}(C_4)| = 32$.

C_5: τ_1 = identity, $\tau_2 = \pi[1,1,3,6]$. $S_1(C_5) = [9]$, $S_2(C_5) = [6,6,6]$, and $|\mathrm{Aut}(C_5)| = 36$.

C_6: $\tau_1 = \pi[1,4,4,4]$, $\tau_2 = \pi[1,4,5,6]$. $S_1(C_6) = [6]$ and $|\mathrm{Aut}(C_6)| = 36$.

C_7: $\tau_1 = \pi[1,1,3,2]$, $\tau_2 = \pi[1,2,1,2]$. $S_1(C_7) = []$, $S_2(C_7) = [27]$ and $|\mathrm{Aut}(C_7)| = 648$. Code C_7 is the only code that is split in more than one coordinate – in coordinates 1 and 5.

C_8: $\tau_1 = \pi[1,1,1,5]$, $\tau_2 = \pi[1,4,5,6]$. $S_1(C_8) = [7]$ and $|\mathrm{Aut}(C_8)| = 8$.

C_9: $\tau_1 = \pi[1,4,4,4]$, $\tau_2 = \pi[1,4,5,2]$. $S_1(C_9) = [4]$ and $|\mathrm{Aut}(C_9)| = 2$.

C_{10}: $\tau_1 = \pi[1,4,4,2]$, $\tau_2 = \pi[1,1,2,3]$. $S_1(C_{10}) = [2]$ and $|\mathrm{Aut}(C_{10})| = 4$.

C_{11}: $\tau_1 = \pi[1,1,1,5]$, $\tau_2 = \pi[1,1,3,2]$. $S_1(C_{11}) = [3]$, $S_2(C_{11}) = [12,6,3,3]$, and $|\mathrm{Aut}(C_{11})| = 6$.

C_{12}: $\tau_1 = \pi[1,1,3,6]$, $\tau_2 = \pi[1,2,1,2]$. $S_1(C_{12}) = []$, $S_2(C_{12}) = [15,6,6]$, and $|\mathrm{Aut}(C_{12})| = 12$.

C_{13}: $\tau_1 = \pi[1,4,5,2]$, $\tau_2 = \pi[4,4,1,3]$. $S_1(C_{13}) = [3]$, $S_2(C_{13}) = [6,6,6,6]$, and $|\mathrm{Aut}(C_{13})| = 48$.

C_{14}: $\tau_1 = \pi[1,1,5,5]$, $\tau_2 = \pi[1,4,1,4]$. $S_1(C_{14}) = [3]$, $S_2(C_{14}) = [6,6,6,6]$, and $|\mathrm{Aut}(C_{14})| = 6$.

C_{15}: $\tau_1 = \pi[1,1,5,3]$, $\tau_2 = \pi[1,4,1,2]$. $S_1(C_{15}) = [1]$ and $|\mathrm{Aut}(C_{15})| = 2$.

C_{16}: $\tau_1 = \pi[1,1,3,3]$, $\tau_2 = \pi[4,1,4,6]$. $S_1(C_{16}) = []$, $S_2(C_{16}) = [9,6,6,6]$, and $|\mathrm{Aut}(C_{16})| = 18$.

C_{17}: $\tau_1 = \pi[1,1,1,2]$, $\tau_2 = \pi[1,1,2,3]$. $S_1(C_{17}) = []$, $S_2(C_{17}) = [9,9,9]$, and $|\mathrm{Aut}(C_{17})| = 54$.

Note that $S_1(C) = []$ implies that the minimum distance of C is greater than 1. Hence codes C_7, C_{12}, C_{16}, and C_{17} have minimum distance 2; all other codes have minimum distance 1. Two of the codes, C_1 and C_7, are equivalent to linear codes.

References

[1] Blass, U.; Litsyn, S.: *Several new lower bounds on the size of codes with covering radius one.* IEEE Trans. Inform. Theory **44** (1998), 1998–2002. Zbl 0932.94038

[2] Cohen, G.; Honkala, I.; Litsyn, S.; Lobstein, A.: *Covering Codes.* North-Holland, Amsterdam 1997. Zbl 0874.94001

[3] Kamps, H. J. L.; van Lint, J. H.: *The football pool problem for 5 matches.* J. Combin. Theory **3** (1967), 315–325. Zbl 0153.32602

[4] Kolev, E.: *Codes over $GF(3)$ of length 5, 27 codewords, and covering radius 1.* J. Combin. Des. **1** (1993), 265–275. Zbl 0924.94036

[5] McKay, B. D.: *nauty user's guide (version 1.5).* Tech. Rep. TR-CS-90-02, Computer Science Department, Australian National University 1990.

[6] Östergård, P. R. J.; Blass, U.: *On optimal binary codes of length 9 and covering radius 1.* IEEE Trans. Inform. Theory, to appear.

[7] Östergård, P. R. J.; Weakley, W. D.: *Classification of binary covering codes.* J. Combin. Des. **8** (2000), 391–401. Zbl pre01558149

[8] Stanton, R. G.; Kalbfleisch, J. G.: *Intersection inequalities for the covering problem.* SIAM J. Appl. Math. **17** (1969), 1311–1316. Zbl 0188.04101

Received January 17, 2001