Since

$$t_3[21,\ 10] \le t_3[20,\ 10] + 1 = 5$$
$$t_3[22,\ 10] \le t_3[21,\ 10] + 1 = 6$$
$$t_3[25,\ 12] \le t_3[24,\ 12] + 1 = 6$$

by bound (2), it follows that $t_3[21,\ 10] = 5$, $t_3[22,\ 10] = 5 - 6$, and $t_3[25,\ 12] = 5 - 6$.

It follows from $t_3[20,\ 11] \le t_3[20,\ 10]$ using (3) that $t_3[20, 11] = 4$.

Using bound (4) $t_3[25, 13] \le t_3[24, 12]$ and, therefore, $t_3[25, 13] = 5$;$t_3[22,\ 11] \le t_3[21,\ 10]$ and thus $t_3[22,\ 11] = 5$ and $t_3[21,\ 11] \le t_3[20,\ 10]$ and, therefore, $t_3[21,\ 11] = 4$.

ACKNOWLEDGMENT

The author wishes to thank Prof. M. Bossert for his hospitality. The author also wishes to thank the anonymous referee for careful reading of the manuscript and for helpful comments and suggestions. This work was done during the visit of the author at Ulm University, Germany.

REFERENCES

[1] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North-Holland, Elsevier Science B.V., 1997.

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

[3] E. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.

[4] F. R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Inform. Theory*, vol. 38, pp. 227–246, Mar. 1992.

[5] E. Velikova, "Bounds on the covering radius of linear codes," *C. R. l'Acad. Bulg. des Sci.*, vol. 41, pp. 13–16, 1988.

[6] H. Mattson Jr., "An improved upper bound on covering radius," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1986, pp. 90–106.

[7] T. Baicheva and E. Velikova, "Covering radii of ternary linear codes of small dimensions and codimensions," *IEEE Trans. Inform. Theory*, vol. 43, pp. 2057–2061, Nov. 1997.

Linear Codes with Covering Radius $R = 2$, 3 and Codimension tR

Alexander A. Davydov and Patric R. J. Östergård, *Member, IEEE*

***Abstract*—Let $[n,\ n-r]_qR$ denote a linear code over F_q with length n, codimension r, and covering radius R. We use a modification of constructions of $[2q+1,\ 2q-3]_q2$ and $[3q+1,\ 3q-5]_q3$ codes ($q \ge 5$) to produce infinite families of good codes with covering radius 2 and 3 and codimension tR.**

***Index Terms*—Bounds on codes, covering code, lengthening, linear code, projective geometry.**

I. INTRODUCTION

We denote the finite field of size q by F_q, where q is a prime power, and vectors of length n with elements from F_q by F_q^n. Moreover, $F_q^* = F_q \backslash \{0\}$. A linear code in F_q^n with dimension k (so the codimension is $r = n - k$) and covering radius R is said to be an $[n,\ k]_qR$ code. If a code has covering radius R, then all words in F_q^r can be obtained as a linear combination of at most R columns of its parity check matrix. The minimum length n such that an $[n,\ k = n - r]_qR$ code exists is denoted by $l(r,\ R;\ q)$. For a survey of covering codes, see [3].

If $R' \le R$ and all words in F_q^r can be obtained as a linear combination with nonzero coefficients of at least R' columns of the parity check matrix of an $[n,\ k]_qR$ code, we say that it is an $[n,\ k]_qR,\ R'$ code. If all words except the all-zero word can be obtained in this way, we say that it is an $[n,\ k]_qR(R')$ code. Respective partitions of the columns such that a required linear combination can always be obtained with the columns belonging to different subsets are called $(R,\ R')$-partitions and $R(R')$-partitions.

Earlier work on linear covering codes has mainly concerned binary codes and q-ary codes with covering radius 2; see [3, Chs. 5 and 7]. Ternary codes with covering radius 3 are considered in [1], [4], [9], and short codes with covering radius 3 over various fields are considered in [7].

In this work, codes over arbitrary fields $q \ge 5$ with $R = 2$ and $R = 3$ are studied. Using a modification of earlier constructions of $[2q + 1,\ 2q - 3]_q2$ and $[3q + 1,\ 3q - 5]_q3$ codes, lengthening constructions are applied to obtain infinite families of good codes of codimension tR. Some special properties of the starting codes make these lengthening constructions effective.

Some matrices with special properties are studied in Section II. The matrices are used as building blocks to construct $[2q + 1,\ 2q - 3]_q2$ and $[3q+1,\ 3q-5]_q3$ codes in Section III. These codes have the same main parameters as codes constructed earlier in [2], [4], [7], but they also have some interesting partitioning properties. These properties are necessary in applying the lengthening constructions that are discussed in Sections IV and V. Infinite families of codes improving on the results in the literature are then obtained. An updated table of $l(r,\ 2;\ 7)$ is given for $r \le 24$.

Manuscript received July 6, 1999; revised November 11, 1999. This work was supported by the Academy of Finland under Grant 44517.

A. A. Davydov is with the Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia (e-mail: adav@iitp.ru).

P. R. J. Östergård is with the Department of Computer Science and Engineering, Helsinki University of Technology, P.O. Box 5400, 02015 HUT, Finland (e-mail: patric.ostergard@hut.fi).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)00597-1.

II. Matrices with Special Properties

In the constructions to be presented we will make use of $3 \times (q+1)$ matrices $\boldsymbol{M}$ that have some special properties. These are as follows.

- P1. The first two lines of the matrix constitute a parity check matrix of the $[q+1,\ q-1]_q 1$ Hamming code.
- P2. All words in F_q^3, except possibly for those of the form $(0,\ 0,\ a)$, can be obtained as a linear combination of at most two columns of $\boldsymbol{M}$.
- P3. Every column of $\boldsymbol{M}$ can be obtained as a linear combination with nonzero coefficients of two other columns of $\boldsymbol{M}$.

A code fulfilling all three properties is said to have property P. From property P3 it follows that in proving property P2 we need only consider words in F_q^3 that are not columns of $\boldsymbol{M}$. Property P3 immediately leads to a few additional properties that will be useful.

Lemma 1: Let $q \geq 4$. If P3 holds, then every column $\boldsymbol{h}$ of $\boldsymbol{M}$ can be obtained as a linear combination with nonzero coefficients of three columns of $\boldsymbol{M}$ (one of which may coincide with $\boldsymbol{h}$), and every combination of two columns, $\boldsymbol{h}$ and $\boldsymbol{h}'$, can be obtained as a linear combination with nonzero coefficients of three different columns of $\boldsymbol{M}$ (two of which may coincide with $\boldsymbol{h}$ and $\boldsymbol{h}'$).

Proof: We have $\boldsymbol{h} = a\boldsymbol{h}_1 + b\boldsymbol{h}_2$, where $a,\ b \in F_q^*$ and $\boldsymbol{h}$, $\boldsymbol{h}_1$, and $\boldsymbol{h}_2$ are different columns of $\boldsymbol{M}$. Then $c\boldsymbol{h} = ca\boldsymbol{h}_1 + cb\boldsymbol{h}_2$ with $c \in F_q^* \backslash \{1\}$ (there are such values when $q \geq 3$) and

$$\boldsymbol{h} = c\boldsymbol{h} + (1-c)a\boldsymbol{h}_1 + (1-c)b\boldsymbol{h}_2$$

and the first property is proved.

From $c\boldsymbol{h} = ca\boldsymbol{h}_1 + cb\boldsymbol{h}_2$, we get

$$c\boldsymbol{h} + c'\boldsymbol{h}' = ca\boldsymbol{h}_1 + cb\boldsymbol{h}_2 + c'\boldsymbol{h}' \qquad (c' \in F_q^*)$$

and we are done unless $\boldsymbol{h}' = \boldsymbol{h}_1$ or $\boldsymbol{h}' = \boldsymbol{h}_2$. Without loss of generality, assume that $\boldsymbol{h}' = \boldsymbol{h}_1$. Then, for all $d \in F_q^*$, $da\boldsymbol{h}' + db\boldsymbol{h}_2 - d\boldsymbol{h} = 0$, so

$$\begin{aligned} c\boldsymbol{h} + c'\boldsymbol{h}' &= c\boldsymbol{h} + c'\boldsymbol{h}' + (da\boldsymbol{h}' + db\boldsymbol{h}_2 - d\boldsymbol{h}) \\ &= (c-d)\boldsymbol{h} + (c' + da)\boldsymbol{h}' + db\boldsymbol{h}_2. \end{aligned}$$

We have a desired solution if $d \neq c$ and $d \neq -a^{-1}c'$. We can always find such a value of d when $q \geq 4$. □

We will now give explicit constructions of matrices that fulfill P1, P2, and P3 for various field parameters. In all these constructions, the columns of the matrices are obtained by taking the points of an oval or hyperoval and slightly modifying a few of these. It is trivial to see that P1 holds, so we do not mention this in the proofs. We study three different cases: $q \geq 8$ even, $q \geq 9$ odd, and $q = 5,\ 7$.

Theorem 1: Let $q = 2^i$ with $i \geq 3$, and let $b \in F_q^* \backslash \{1\}$ such that $b^2 + b + 1 \neq 0$ if i is even. The following matrix over F_q, where $\{a_1, \ldots, a_{q-2}\} = F_q \backslash \{1,\ b\}$, has property P:

$$\left[\begin{array}{ccc|ccc} 1 & \cdots & 1 & 0 & 1 & 1 \\ a_1 & \cdots & a_{q-2} & 1 & 1 & b \\ a_1^2 & \cdots & a_{q-2}^2 & 1 & 0 & 0 \end{array}\right].$$

Proof: The following linear combinations show that P3 holds:

$$(1,\ a,\ a^2) + (1,\ a+1,\ (a+1)^2) = (0,\ 1,\ 1) \qquad (a \notin \{0,\ 1,\ b,\ b+1\})$$

$$(b+1)(1,\ 0,\ 0) + b(1,\ 1,\ 0) = (1,\ b,\ 0)$$

and

$$(1,\ b+1,\ (b+1)^2) + b^2(1,\ (b+1)/b,\ (b+1)^2/b^2) = (b^2+1)(1,\ 1,\ 0).$$

In the last linear combination we must have $(b+1)/b \neq b$, that is, $b^2 + b + 1 \neq 0$. By taking the trace relative to the subfield F_2, we get $\mathrm{Tr}\,(b^2 + b + 1) = \mathrm{Tr}(1)$. If i is odd, then $\mathrm{Tr}\,(1) = 1$, and there are no solutions. If i is even, then $b^2 + b + 1 = 0$ has two solutions. However, as $q \geq 8$, we can always find appropriate values of b.

To prove P2, we use the fact that the matrix is obtained by taking a hyperoval, deleting four points, and finally adding three points. It is well known [8, Sec. 8.1] that every point outside a hyperoval lies on exactly $q/2 + 1$ bisecants of the hyperoval, and thus on at least $q/2 - 3$ bisecants of a hyperoval with four points deleted. This number is positive if $q \geq 8$. We must finally consider the points that were deleted from the hyperoval, except for $(0, 0, 1)$

$$(1,\ 0,\ 0) + (0,\ 1,\ 1) = (1,\ 1,\ 1)$$

$$(1,\ 1,\ 0) + (1,\ 0,\ 0) = (0,\ 1,\ 0)$$

and

$$(1,\ b+1,\ (b+1)^2) + (0,\ 1,\ 1) = (1,\ b,\ b^2).$$ □

Theorem 2: Let $q \geq 9$ be odd and let $b \in F_q^* \backslash \{1,\ -1,\ 1/2\}$. The following matrix over F_q, where $\{a_1, \ldots, a_{q-2}\} = F_q \backslash \{b,\ 1-b\}$, has property P:

$$\left[\begin{array}{ccc|ccc} 1 & \cdots & 1 & 1 & 1 & 0 \\ a_1 & \cdots & a_{q-2} & b & 1-b & 1 \\ a_1^2 & \cdots & a_{q-2}^2 & 0 & b^2 & 0 \end{array}\right].$$

Proof: The following linear combinations show that P3 holds:

$$(1,\ a,\ a^2) - (1,\ -a,\ a^2) = 2a(0,\ 1,\ 0) \qquad (a \notin \{0,\ b,\ -b,\ b-1,\ 1-b\})$$

$$(1,\ 0,\ 0) + b(0,\ 1,\ 0) = (1,\ b,\ 0)$$

$$(1,\ 1-b,\ b^2) - (1,\ -b,\ b^2) = (0,\ 1,\ 0)$$

and

$$b^2(1,\ -(1-b),\ (1-b)^2) + (1-b^2)(1,\ b,\ 0) = (1,\ b(1-b),\ b^2(1-b)^2).$$

To prove P2, note that the matrix is obtained by taking an oval, deleting three points, and adding three points. Since every point outside an oval lies on at least $(q-1)/2$ bisecants of the oval [8, Table 8.2], such points are on at least $(q-1)/2-3$ bisecants after three points are deleted. This number is positive if $q \geq 9$. We finally consider the points that were deleted from the oval, except for $(0,\ 0,\ 1)$

$$(1,\ -(1-b),\ (1-b)^2) + 2(1-b)(0,\ 1,\ 0) = (1,\ 1-b,\ (1-b)^2)$$

and

$$(1,\ -b,\ b^2) + 2b(0,\ 1,\ 0) = (1,\ b,\ b^2).$$ □

We finally consider the case $q = 5,\ 7$ and state the following theorem without proof. (The theorem is easily checked by computer or, with some patience, by hand.)

Theorem 3: The following two matrices over F_5 and F_7, respectively, have property P:

$$\left[\begin{array}{cccc|cc} 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 3 & 4 & 2 & 1 \\ 0 & 1 & 4 & 1 & 0 & 0 \end{array}\right]$$

$$\left[\begin{array}{cccccc|cc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 3 & 4 & 5 & 6 & 2 & 1 \\ 0 & 1 & 2 & 2 & 4 & 1 & 0 & 0 \end{array}\right].$$

III. Codes of Length $qR + 1$ and Codimension $2R$

We will now present the codes that will be the seeds for the infinite families of covering codes to be constructed. In the sequel, $\boldsymbol{O}_1$ denotes

a matrix from Theorem 1 ($q \geq 8$ even), Theorem 2 ($q \geq 9$ odd), or Theorem 3 ($q = 5, 7$), and $\boldsymbol{O}_2$ denotes such a matrix with the rows in reverse order. Moreover, $\boldsymbol{L}_1$ denotes the $2 \times q$ matrix

$$\begin{bmatrix} 0 & 1 & \cdots & 1 \\ 1 & a_1 & \cdots & a_{q-1} \end{bmatrix}$$

where $\{a_1, \ldots, a_{q-1}\} = F_q^*$, and $\boldsymbol{L}_2$ is obtained by deleting the first column of $\boldsymbol{L}_1$. It is necessary to prove the following property of matrices $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$.

Theorem 4: Let $q \geq 4$. Every column of $\boldsymbol{L}_1$ (respectively, $\boldsymbol{L}_2$) can be obtained as a linear combination with nonzero coefficients of two other columns of $\boldsymbol{L}_1$ ($\boldsymbol{L}_2$).

Proof: The columns of $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$ can be seen as subsets of points on a line in the projective geometry PG$(1, q)$. The required linear combination exists if we have at least three distinct points on the line, that is, if $q - 1 \geq 3$. □

The main constructions are now as follows:

$$\boldsymbol{M}_1 = \begin{array}{|c|c|} \hline \boldsymbol{O}_1 & \\ \hline & \boldsymbol{L}_1 \\ \hline \end{array} \qquad (1)$$

$$\boldsymbol{M}_2 = \begin{array}{|c|c|c|} \hline \boldsymbol{O}_1 & & \\ \hline & \boldsymbol{L}_2 & \\ \hline & & \boldsymbol{O}_2 \\ \hline \end{array} \qquad (2)$$

The matrices $\boldsymbol{M}_1$ (1) and $\boldsymbol{M}_2$ (2) are of size $4 \times (2q + 1)$ and $6 \times (3q + 1)$, respectively. The unmarked areas of the matrices contain zeros. The sizes of these areas can easily be calculated from the sizes of the marked areas, which are $3 \times (q + 1)$ ($\boldsymbol{O}_i$), $2 \times q$ ($\boldsymbol{L}_1$), and $2 \times (q - 1)$ ($\boldsymbol{L}_2$). For example, the unmarked areas of $\boldsymbol{M}_1$ are of size $1 \times (q + 1)$ and $2 \times q$.

Theorem 5: $\boldsymbol{M}_1$ is a parity check matrix of a $[2q + 1, 2q - 3]_q 2(2)$ code $(q \geq 5)$.

Proof: We need only prove that the code is a $[2q + 1, 2q - 3]_q 2$ code, since due to Theorems 1, 2, 3, and 4, it will then follow that it is a $[2q + 1, 2q - 3]_q 2(2)$ code.

We consider a vector $(a, b, c, d) \in F_q^4$. The case with $a = b = 0$ is taken care of by $\boldsymbol{L}_1$. If either $a \neq 0$ or $b \neq 0$, we get two subcases. If $d = 0$, the theorem follows from property P2 of $\boldsymbol{O}_1$. If $d \neq 0$, due to property P1, there is a column of $\boldsymbol{O}_1$ a multiple of which can be subtracted from (a, b, c, d) to get $(0, 0, c', d)$. Remembering that now $d \neq 0$, this is a multiple of a column of $\boldsymbol{L}_1$. □

We will now give possible $2(2)$-partitions for these $[2q + 1, 2q - 3]_q 2(2)$ codes with $q \geq 7$, which will be used later. We consider three cases: $q = 7$, $q \geq 8$ even, and $q \geq 9$ odd. In all cases, $S_1 \cup S_2$ denotes a partition of the columns of $\boldsymbol{L}_i$ such that $|S_1| \geq 2$ and $|S_2| \geq 2$.

The partitions are given without proofs. Their correctness follows from the proofs of Theorems 1, 2, and 5 with a few additional arguments. For example, if a subset of a partition consists of $u \geq 2$ points of an oval then all bisecants through two points of this subset are "lost" for covering and we subtract $\lfloor u/2 \rfloor$ from the total number of bisecants on which every point outside the oval lies. The partition for $q = 7$ can be checked by computer or by hand.

$q = 7$: One possible partition into eight subsets is

$$\begin{aligned} &S_1 \cup S_2 \cup \{(1, 0, 0, 0), (0, 1, 0, 0)\} \\ &\quad \cup \{(1, 1, 1, 0)\} \cup \{(1, 3, 2, 0)\} \cup \{(1, 4, 2, 0)\} \\ &\quad \cup \{(1, 5, 4, 0)\}) \cup \{(1, 6, 1, 0), (1, 2, 0, 0)\}. \end{aligned}$$

$q \geq 8$ even: Let T_j, $j = 0, 1$, be the sets of columns of form $(1, a, a^2, 0)$ with $a \in F_q \backslash \{0, 1, b, b + 1\}$, where a transformation of a into binary representation has a j in its last position. Moreover, let $T_j = T_j' \cup T_j''$ be any partition of T_j such that $|T_j'| = |T_j''|$. We have $|T_j'| = (q - 4)/4$ where $(q - 4)/4$ is odd. One possible partition into nine subsets is then

$$\begin{aligned} &S_1 \cup S_2 \cup \{(0, 1, 1, 0)\} \cup \{(1, 0, 0, 0)\} \\ &\quad \cup \{(1, b + 1, (b + 1)^2, 0)\} \cup (T_0' \cup \{(1, b, 0, 0)\}) \\ &\quad \cup (T_0'' \cup \{(1, 1, 0, 0)\}) \cup T_1' \cup T_1''. \end{aligned}$$

$q \geq 9$ odd: The columns of the form $(1, a, a^2, 0)$ with $a \in F_q \backslash \{0, b, -b, 1 - b, b - 1\}$ are partitioned into two sets U_1 and U_2, such that $(1, a, a^2, 0)$ and $(1, -a, a^2, 0)$ belong to different sets for all a. Then $|U_1| = |U_2| = (q - 5)/2$. The sets U_1 and U_2 are further partitioned $U_1 \cup U_2 = V_1 \cup V_2 \cup V_3 \cup V_4$ so that $|V_i|$ is odd for all i. (That is, if $|U_i|$ is even, both sets are split into two sets, otherwise, one set is split into three sets.) One possible partition into 12 subsets is then

$$\begin{aligned} &S_1 \cup S_2 \cup V_1 \cup V_2 \cup V_3 \cup V_4 \cup \{(0, 1, 0, 0)\} \\ &\quad \cup \{(1, b, 0, 0)\} \cup \{(1, 1 - b, b^2, 0)\} \cup \{(1, 0, 0, 0)\} \\ &\quad \cup \{(1, -(1 - b), (1 - b)^2, 0)\}) \cup \{(1, -b, b^2, 0)\}. \end{aligned}$$

Theorem 6: $\boldsymbol{M}_2$ is a parity check matrix of a $[3q + 1, 3q - 5]_q 3, 3$ code $(q \geq 5)$.

Proof: In this case, we need only prove that the code is a $[3q + 1, 3q - 5]_q 3$ code, after which Theorems 1, 2, 3, and 4, and Lemma 1 give that it is a $[3q + 1, 3q - 5]_q 3, 3$ code.

The proof that $\boldsymbol{M}_2$ is a $[3q + 1, 3q - 5]_q 3$ code is essentially the same as that of [7, Theorem 7]. Note that the symmetries of matrices $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ impose a symmetry on $\boldsymbol{M}_2$. We leave the details of this case-by-case proof, which can also be seen as an extension of the proof of Theorem 5, to the reader. □

As we will see in the next section, the $(3, 3)$-partitions play a minor role in the constructions to be presented, and this issue will then be touched just briefly.

IV. Lengthening Constructions for $R = 2$

The following construction of codes with covering radius 2 is considered in [5], [6]. We start from an $[n, n - r]_q 2(2)$ code with parity check matrix $\boldsymbol{H} = [\boldsymbol{h}_1 \ \boldsymbol{h}_2 \ \cdots \ \boldsymbol{h}_n]$. The parity check matrix of the new code is $\boldsymbol{H}_2 = [\boldsymbol{H}_{2,1} \ \boldsymbol{H}_{2,2}]$ (see the bottom of the next page), where $n' < n$, α is a primitive element in F_{q^m}, and the values β_i are elements in F_{q^m} on which some further restrictions will be imposed. It is required that $\boldsymbol{h}_{n'}, \ldots, \boldsymbol{h}_n$ all belong to the same subset in the $2(2)$-partition. To get a matrix over F_q, the elements of the last two rows are mapped to m-element columns over F_q. The following theorem, which also tells how m should be chosen, is [6, Theorem 3].

Theorem 7: If $\boldsymbol{H}$ is a parity check matrix of an $[n, n - r]_q 2(2)$ code having a $2(2)$-partition into N subsets, $N \leq q^m + 1 \leq n$, if $\beta_i \neq \beta_j$ when $\boldsymbol{h}_i$ and $\boldsymbol{h}_j$ belong to different subsets in this $2(2)$-partition, and if $\cup_{i=1}^{n'-1} \{\beta_i\} = F_{q^m}$, then $\boldsymbol{H}_2$ is a parity check matrix for an

TABLE I
UPPER BOUNDS ON $l(r,\ 2;\ 7)$ FOR $r \leq 24$

r	$l(r,2;7)$	Reference	N	r_0	μ	r	$l(r,2;7)$	Reference	N	r_0	μ
3	6	[8]			1.683	14	252105	Theorem 7	64	10	1.687
4	15	Theorem 5	8		1.613	15	741909	[5]			2.087
5	44	[5]			2.042	16	1764735	Theorem 7	64	10	1.687
6	105	Theorem 7	16	4	1.676	17	5193363	[5]			2.087
7	309	[5]			2.083	18	12353145	Theorem 7	64	10	1.687
8	743	Theorem 10	9	4	1.723	19	36353541	[5]			2.087
9	2164	[5]			2.089	20	86472015	Theorem 7	128	14	1.687
10	5145	Theorem 7	32	6	1.687	21	254474787	[5]			2.087
11	15141	[5]			2.087	22	605304105	Theorem 7	128	14	1.687
12	36407	Theorem 7	18	8	1.724	23	1781323509	[5]			2.087
13	106036	[5]			2.089	24	4237128735	Theorem 7	128	14	1.687

$[n'' = nq^m,\ n'' - (2m + r)]_q 2(2)$ code having a $2(2)$-partition into $2N$ subsets.

Our starting code from Theorem 5 has length $2q + 1$, so in applying Theorem 7, $q^m + 1 \leq n = 2q + 1$ implies that $m = 1$. Moreover, we must have $N \leq q^m + 1$, so with $m = 1$ we get $N \leq q + 1$. Using the partitions from the previous section, we are able to apply this theorem when $q = 7$, $q \geq 8$ even, and $q \geq 11$ odd.

Having applied Theorem 7, we get a code to which we can apply the same theorem again. The following general theorem, which is a part of [6, Theorem 4], shows that we then get an infinite family of codes.

Theorem 8: Let $q \geq 3$. If Theorem 7 can be applied to an $[n_0,\ n_0 - r_0]_q 2(2)$ code with $m_0 = 1$, then $l(r_0 + 2m,\ 2;\ q) \leq n_0 q^m$ for all $m \geq 10$.

Theorem 8 applied to the seeds constructed in this correspondence gives that $l(2t,\ 2;\ q) \leq 2q^{t-1} + q^{t-2}$ for $t \geq 12$ and $q = 7,\ 8$, $q \geq 11$, which improves on [5, Example 5]. Clearly, $l(2t,\ 2;\ q) \leq 2q^{t-1} + q^{t-2}$ for several values $t < 12$; we shall now try to find such values of t.

Using Theorem 7 on the code of Theorem 6, we get an $[n = 2q^2 + q,\ n - 6]_q 2(2)$ code $\mathcal{C}_1$ with $N \leq 2q + 2$. For $\mathcal{C}_1$ we apply Theorem 7 with $m = 2$ and get an $[n = 2q^4 + q^3,\ n - 10]_q 2(2)$ code $\mathcal{C}_2$ with $N \leq 4q + 4$. Then for $\mathcal{C}_2$ we use Theorem 7 with $m = 2,\ 3,\ 4$, and get an $[n = 2q^6 + q^5,\ n - 14]_q 2(2)$ code $\mathcal{C}_3$ with $N \leq 8q + 8$ and codes with $t = 8,\ 9$. Finally, for $\mathcal{C}_3$ we apply Theorem 7 with $m = 3,\ 4$ and get codes with $t = 10,\ 11$. The results obtained by applying Theorems 7 and 8 to the seeds of Theorem 6 are summarized in the next theorem.

Theorem 9: $l(2t,\ 2;\ q) \leq 2q^{t-1} + q^{t-2}$ for $t = 2,\ 3,\ 5, t \geq 7$ and $q = 7,\ 8, q \geq 11$.

To get an upper bound for $t = 4$ and $t = 6$ one may apply the following theorem, which is a part of [6, Theorem 2].

Theorem 10: Let $q \geq 3$. If an $[n_0,\ n_0 - r_0]_q 2(2)$ code having a $2(2)$-partition into $N \leq q^m$ subsets exists, then an

$$[n = n_0 q^m + (q^m + 1)/(q - 1),\ n - (2m + r_0)]_q 2(2)$$

code having a $2(2)$-partition into $N + 1$ subsets exists as well.

For $\mathcal{C}_1$ we apply Theorem 10 with $m = 2$ and get an

$$[n = 2q^3 + q^2 + q + 1,\ n - 8]_q 2(2)$$

code $\mathcal{C}'$ with $N \leq q + 2$. Finally, for $\mathcal{C}'$ we apply Theorem 7 with $m = 2$ and get an

$$[n = 2q^5 + q^4 + q^3 + q^2,\ n - 12]_q 2(2)$$

code.

The result in Theorem 9 can be compared with a construction in [5, Example 5] that gives an infinite family of codes with length $2q^{t-1} + q^{t-2} + q^{t-3}$ for $q \geq 4$ and $t = 3,\ 5$, and for $q \geq 5$ and $t \geq 7$.

We shall now see how the code families given by Theorem 9 behave asymptotically with the codimension and length going to infinity. A good parameter in judging the quality of a code is its *density*. The density is defined as the average number of codewords that are at distance less than or equal to R, the covering radius, from any word in the space. The density of the code families is

$$\mu = 2 - \frac{2}{q} - \frac{3}{2q^2} + \frac{1}{q^3} + \frac{1}{2q^4} + O(q^{-t+1}).$$

$$\boldsymbol{H}_{2,1} = \left[\begin{array}{cccc|c|cccc} \boldsymbol{h}_1 & \boldsymbol{h}_1 & \cdots & \boldsymbol{h}_1 & \cdots & \boldsymbol{h}_{n'-1} & \boldsymbol{h}_{n'-1} & \cdots & \boldsymbol{h}_{n'-1} \\ 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q^m-2} \\ 0 & \beta_1\alpha^0 & \cdots & \beta_1\alpha^{q^m-2} & \cdots & 0 & \beta_{n'-1}\alpha^0 & \cdots & \beta_{n'-1}\alpha^{q^m-2} \end{array}\right]$$

$$\boldsymbol{H}_{2,2} = \left[\begin{array}{cccc|c|cccc} \boldsymbol{h}_{n'} & \boldsymbol{h}_{n'} & \cdots & \boldsymbol{h}_{n'} & \cdots & \boldsymbol{h}_n & \boldsymbol{h}_n & \cdots & \boldsymbol{h}_n \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q^m-2} \end{array}\right]$$

$$\boldsymbol{H}_{3,1} = \left[\begin{array}{cccc|c|ccc} \boldsymbol{h}_1 & \boldsymbol{h}_1 & \cdots & \boldsymbol{h}_1 & \cdots & \boldsymbol{h}_{n'-1} & \boldsymbol{h}_{n'-1} & \cdots & \boldsymbol{h}_{n'-1} \\ 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q^m-2} \\ 0 & \beta_1\alpha^0 & \cdots & \beta_1\alpha^{q^m-2} & \cdots & 0 & \beta_{n'-1}\alpha^0 & \cdots & \beta_{n'-1}\alpha^{q^m-2} \\ 0 & \beta_1^2\alpha^0 & \cdots & \beta_1^2\alpha^{q^m-2} & \cdots & 0 & \beta_{n'-1}^2\alpha^0 & \cdots & \beta_{n'-1}^2\alpha^{q^m-2} \end{array}\right]$$

$$\boldsymbol{H}_{3,2} = \left[\begin{array}{cccc|c|ccc} \boldsymbol{h}_{n'} & \boldsymbol{h}_{n'} & \cdots & \boldsymbol{h}_{n'} & \cdots & \boldsymbol{h}_{n''-1} & \boldsymbol{h}_{n''-1} & \cdots & \boldsymbol{h}_{n''-1} \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q^m-2} \end{array}\right]$$

$$\boldsymbol{H}_{3,3} = \left[\begin{array}{cccc|c|cccc} \boldsymbol{h}_{n''} & \boldsymbol{h}_{n''} & \cdots & \boldsymbol{h}_{n''} & \cdots & \boldsymbol{h}_n & \boldsymbol{h}_n & \cdots & \boldsymbol{h}_n \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q^m-2} \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right]$$

We get the asymptotic densities $1.687, 1.729$, and 1.807 for $q = 7, 8$, and 11, respectively. We finally give an updated table of upper bounds on $l(r, 2; 7)$ for $r \leq 24$ based on the results of this section. Comparing with [5, Table I], the results in this correspondence lead to improvements for all even codimensions $r \geq 6$. The column N in Table I gives the number of subsets in a $(2, 2)$-partition obtained by the construction used, r_0 gives the codimension of the code from which it was constructed, and μ gives the density of the code.

V. Lengthening Constructions for $R = 3$

We will now consider constructions for $R = 3$. We start from an $[n, n-r]_q 3, 3$ code with parity check matrix $\boldsymbol{H} = [\boldsymbol{h}_1\ \boldsymbol{h}_2\ \cdots\ \boldsymbol{h}_n]$. The parity check matrix of the new code is $\boldsymbol{H}_3 = [\boldsymbol{H}_{3,1}\ \boldsymbol{H}_{3,2}]$ for odd q and $\boldsymbol{H}'_3 = [\boldsymbol{H}_{3,1}\ \boldsymbol{H}_{3,2}\ \boldsymbol{H}_{3,3}]$ for even q (see the top of the following page), where $n' < n''$, $n'' < n$ ($n''-1 = n$ for q odd), α is a primitive element in F_{q^m}, and the values β_i are elements in F_{q^m} on which some further restrictions will be imposed. It is required that $\boldsymbol{h}_{n'}, \ldots, \boldsymbol{h}_{n''-1}$ all belong to the same subset in the $(3, 3)$-partition, and the same holds for $\boldsymbol{h}_{n''}, \ldots, \boldsymbol{h}_n$. To get a matrix over F_q, the elements of the last three rows are mapped to m-element columns over F_q.

Theorem 11: If q is odd (even) and $\boldsymbol{H}$ is a parity check matrix of an $[n, n-r]_q 3, 3$ code having a $(3, 3)$-partition into N subsets, $N \leq q^m + 1$ ($N \leq q^m + 2$), if $\beta_i \neq \beta_j$ when $\boldsymbol{h}_i$ and $\boldsymbol{h}_j$ belong to different subsets in this $(3, 3)$-partition, then $\boldsymbol{H}_3$ ($\boldsymbol{H}'_3$) is a parity check matrix for an $[n'' = nq^m, n'' - (3m + r)]_q 3, 3$ code.

Proof: Since $\boldsymbol{H}$ is a parity check matrix of an $[n, n-r]_q 3, 3$ code, every column $\boldsymbol{a} \in F_{q^r}$ can be represented as $\boldsymbol{a} = u\boldsymbol{h}_e + v\boldsymbol{h}_f + w\boldsymbol{h}_g$ with $\boldsymbol{h}_e, \boldsymbol{h}_f$, and $\boldsymbol{h}_g$ belonging to different subsets in the $(3, 3)$-partition and $u, v, w \in F_q^*$. We will show that every

$$(\boldsymbol{a}, b, c, d) \in F_{q^r} F_{q^m} F_{q^m} F_{q^m}$$

can be obtained as a linear combination of exactly three columns of $\boldsymbol{H}_3$ ($\boldsymbol{H}'_3$).

We use a projective geometry approach and the fact that an arbitrary point of a projective plane can be obtained as a linear combination using any three points in the plane that are not collinear. For a given $\boldsymbol{h}_i$, the last three rows of $\boldsymbol{H}_3$ ($\boldsymbol{H}'_3$) give a point of the projective geometry PG$(2, q^m)$ with coordinates in all possible homogeneous forms. Moreover, these points are $(1, \beta_i, \beta_i^2)$, $(0, 0, 1)$, and, if q is even, $(0, 1, 0)$. This means that these are points of an oval if q is odd and of a hyperoval if q is even. The fact that no three points of an oval or a hyperoval are collinear settles this case.

Since the all-zero word does not belong to the projective geometry, we have to consider this case separately. We then simply take

$$(\boldsymbol{a}, 0, 0, 0) = u(\boldsymbol{h}_e, 0, 0, 0) + v(\boldsymbol{h}_f, 0, 0, 0) + w(\boldsymbol{h}_g, 0, 0, 0). \quad \square$$

Actually, for our purpose, it is sufficient to know that we get a code with covering radius 3; the additional parameter $R' = 3$ is not essential.

We can now apply Theorem 11 to the code from Theorem 6. Notice that even by using the trivial $(3, 3)$-partition of the code with each column in its own set and $3q + 1$ sets, we are able to apply Theorem 11 whenever $3q + 1 \leq q^m + 1$, that is, for $m \geq 2$.

We should mention, however, that we have found $(3, 3)$-partitions with 17 and 23 sets for the cases $q \geq 8$ even and $q \geq 9$ odd, respectively (in the same way as $2(2)$-partitions were obtained in the previous section). For the $(3, 3)$-partitions, we partition the matrix $\boldsymbol{L}_2$ into three subsets and the matrix $\boldsymbol{O}_2$ in the same way as $\boldsymbol{O}_1$ (remember that $\boldsymbol{O}_1$ and $\boldsymbol{O}_2$ are symmetric). With these partitions, we can apply Theorem 11 with $m = 1$ for $q \geq 16$ even and $q \geq 23$ odd. We summarize the results in the following theorem.

Theorem 12: $l(3t, 3; q) \leq 3q^{t-1} + q^{t-2}$ with $t \geq 4$, $q \geq 5$ (and $t = 3$, $q = 16$, $q \geq 23$).

This result can be compared with [4, Example 7.2], where infinite code families of size

$$3q^{t-1} + 2q^{t-2} + 2q^{t-3} + 2q^{t-4}$$

and

$$3q^{t-1} + 2q^{t-2} + q^{t-3} + q^{t-4} + q^{t-5}$$

are obtained for $q \geq 4$ and $q \geq 8$ even, respectively.

We finally give the asymptotic density for the code families from Theorem 12. It is

$$\mu = \frac{9}{2} - \frac{9}{q} + \frac{3}{2q^2} + \frac{14}{3q^3} - \frac{1}{2q^4} - \frac{1}{q^5} - \frac{1}{6q^6} + O(q^{-t+1}).$$

We get the asymptotic densities $2.797, 3.259, 3.408, 3.525$, and 3.698 for $q = 5, 7, 8, 9$, and 11, respectively.

Acknowledgment

The authors wish to thank the anonymous referees for remarks that helped to improve the correspondence. The first author gratefully acknowledges the Academy of Finland and Helsinki University of Technology (HUT) for hospitality during the visit at HUT.

References

[1] T. S. Baicheva and E. D. Velikova, "Covering radii of ternary linear codes of small dimensions and codimensions," *IEEE Trans. Inform. Theory*, vol. 43, pp. 2057–2061, Nov. 1997.

[2] R. A. Brualdi, V. S. Pless, and R. M. Wilson, "Short codes with a given covering radius," *IEEE Trans. Inform. Theory*, vol. 35, pp. 99–109, Jan. 1989.

[3] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: North–Holland, 1997.

[4] A. A. Davydov, "Constructions and families of covering codes and saturated sets of points in projective geometry," *IEEE Trans. Inform. Theory*, vol. 41, pp. 2071–2080, Nov. 1995.
[5] ——, "Constructions and families of nonbinary linear codes with covering radius 2," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1679–1686, July 1999.
[6] A. A. Davydov and P. R. J. Östergård, "New quaternary linear codes with covering radius 2," *Finite Fields Appl.*, vol. 6, pp. 164–174, 2000.
[7] ——, "On saturating sets in small projective geometries," *European J. Combin.*, vol. 21, pp. 563–570, 2000.
[8] J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, 2nd ed. Oxford, U.K.: Clarendon, 1998.
[9] T. S. Baicheva and E. D. Velikova, "Correction to 'Covering radii of ternary linear codes of small dimensions and codimensions'," *IEEE Trans. Inform. Theory*, vol. 44, p. 2032, Sept. 1998.

On Binary Cyclic Codes with Codewords of Weight Three and Binary Sequences with the Trinomial Property

Pascale Charpin, Aimo Tietäväinen, and Victor Zinoviev

***Abstract*—Golomb and Gong ([8] and [9]) considered binary sequences with the trinomial property. In this correspondence we shall show that the sets of those sequences are (quite trivially) closely connected with binary-cyclic codes with codewords of weight three (which were already studied in [4] and [5]). This approach gives us another way to deal with trinomial property problems. After disproving one conjecture formulated by Golomb and Gong in [9], we exhibit an infinite class of sequences which do not have the trinomial property, corresponding to binary cyclic codes of length 2^m-1 with minimum distance exactly four.**

***Index Terms*—Binary cyclic code, factorization of polynomials, periodic binary sequence, trinomial, trinomial pair.**

I. Introduction

One of the interesting objects of algebraic coding theory is cyclic codes. Many problems connected with these codes are open. Even the simplest case—binary cyclic codes with minimal distance three—is still far from a complete classification (see [4] and [5]). In the recent papers [8] and [9], binary sequences with so-called trinomial properties were considered. We say that a binary sequence $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1})$ of length $n = 2^m - 1$ has the trinomial property if there is (at least) one pair of positive integers, k and ℓ, where $0 < k, \ell < n$, such that

$$a_i + a_{i+k} + a_{i+\ell} = 0$$

for all i, $i \in \{0, 1, \ldots, n-1\}$, where the indices are taken modulo n. The purpose of this correspondence is to set a one-to-one relation between these two problems, i.e., between binary-cyclic codes with the minimal distance three and binary sequences with trinomial properties.

In Section II, we consider binary sequences with trinomial properties and characterize such sequences in terms of cyclic codes with minimal distance three. In Section III, we construct families of such sequences explicitly. Section IV is devoted to disproving the conjecture from [9] that any nonlinear binary sequence of period $n = 2^m - 1$, where m is prime, has no trinomial property. Finally, in Section V, we construct infinite families of binary nonlinear sequences which have no trinomial properties.

In this correspondence, a *codeword* is an element of the vector space F_2^n. A *code* is a subspace of F_2^n. The *distance* between two codewords will always be the Hamming distance. So the weight of any codeword $x = (x_1, \ldots, x_n)$ will be the Hamming weight $\mathrm{wt}\,(x) = \sum_{i=1}^n x_i$. The *dual* of any binary linear code C of length n is defined by means of the standard scalar product

$$C^\perp = \{\, y \in F_2^n \mid z \cdot y = 0, z \in C \,\} \tag{1}$$

where $z \cdot y = \sum_{i=1}^n z_i y_i$, $z = (z_1, \ldots, z_n)$, and $y = (y_1, \ldots, y_n)$.

II. On Binary Sequences with the Trinomial Property

Denote the finite field of order 2^m by F_{2^m}. Let $n = 2^m - 1$ and

$$R_n = F_2[x]/(x^n + 1).$$

In this correspondence, we consider elements of R_n and, as usual, we identify the sequence (or vector)

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}) \in F_2^n$$

and the polynomial

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in R_n.$$

Definition 1 (cf. [8] and [9]): A sequence

$$\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}) \in R_n$$

has the (k, ℓ) trinomial property (or (k, ℓ) is a trinomial pair of $\boldsymbol{a}$), if for any $i \in \{0, 1, \ldots, n-1\}$ we have

$$a_i + a_{i+k} + a_{i+\ell} = 0$$

where the indexes are taken modulo n and k, ℓ are positive integers.

Let us mention that in [8] and [9], Golomb and Gong further assumed that the (smallest) period of $\boldsymbol{a}$ is n.

Define the following sets. For given k and ℓ, $0 < k, \ell < n$, let

$$S(k, \ell) = \{\boldsymbol{a} \in R_n \mid \boldsymbol{a} \text{ has the } (k, \ell) \text{ trinomial property}\}.$$

Since evidently $S(k, k) = \{\boldsymbol{0}\}$ and $S(\ell, k) = S(k, \ell)$, it is natural to define

$$\mathcal{S} = \bigcup \{S(k, \ell) \mid 0 < k < \ell < n\}. \tag{2}$$

Statement 1: $S(k, \ell)$ is a cyclic code (and thus also $S(k, \ell)^\perp$, the dual of $S(k, \ell)$, is cyclic).

Proof: If the vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ have the (k, ℓ) trinomial property, then also their sum $\boldsymbol{a} + \boldsymbol{b}$ has that property. Therefore, the set $S(k, \ell)$ is a linear space. By definition it is cyclic. Thus, $S(k, \ell)$ is a cyclic code. □

Theorem 1: We denote by $\langle h(x) \rangle$ the cyclic code generated by $h(x)$, i.e., the ideal of R_n generated by $h(x)$. Then

$$S(k, \ell) = \langle \gcd\,(1 + x^k + x^\ell, 1 + x^n) \rangle^\perp.$$

Manuscript received February 24, 2000; revised August 15, 2000. The work was supported by the Academy of Finland and by the Russian Fundamental Research Foundation under Project 99-01-00828. The material in this correspondence was presented at the 7th International Workshop on Algebraic and Combinatorial Coding Theory, Blagoevgrad, Bulgaria, June 18–19, 2000.

P. Charpin is with the INRIA-Rocquencourt, Domaine de Voluceau, BP 105, 78153 Le Chesnay, France (e-mail: Pascale.Charpin@inria.fr).

A. Tietäväinen is with the Department of Mathematics and TUCS, University of Turku, FIN-20014 Turku, Finland (e-mail: tietavai@lena.utu.fi).

V. Zinoviev is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi 19, GSP-4, Moscow 101447, Russia (e-mail: zinovev@iitp.ru).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)00373-X.