Designs, Codes and Cryptography, 16, 29–39 (1999)
© 1999 Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

New Linear Codes with Covering Radius 2 and Odd Basis*

ALEXANDER A. DAVYDOV adav@iitp.ras.ru
Institute for Problems of Information Transmission, Russian Academy of Sciences,
Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia

PATRIC R. J. ÖSTERGÅRD patric.ostergard@hut.fi
Department of Computer Science and Engineering, Helsinki University of Technology,
P.O. Box 5400, 02015 HUT, Finland

Communicated by: D. Jungnickel

Received November 25, 1997; Revised March 13, 1998; Accepted September 4, 1998

Abstract. On the way of generalizing recent results by Cock and the second author, it is shown that when the basis q is odd, BCH codes can be lengthened to obtain new codes with covering radius $R = 2$. These constructions (together with a lengthening construction by the first author) give new infinite families of linear covering codes with codimension $r = 2k + 1$ (the case $q = 3$, $r = 4k + 1$ was considered earlier). New code families with $r = 4k$ are also obtained. An updated table of upper bounds on the length function for linear codes with $r \leq 24$, $R = 2$, and $q = 3, 5$ is given.

Keywords: BCH code, covering code, covering radius, finite field, length function

1. Introduction

In a recent paper, Cock and the second author [1] present a construction of linear ternary ($q = 3$) codes with covering radius 2 and a good asymptotic behavior. The codes are constructed starting from BCH codes, which are first extended, and then lengthened by adding columns to the parity check matrix. It is here shown how this construction can be generalized for any odd q to give families of codes with codimension $r = 2k+1$. The new codes obtained are further used in a lengthening construction by the first author [3] to get more new codes.

We use the following notations. In the rest of the paper we assume that q is an odd prime power. Let F_q denote the finite field of order q. We will be particularly interested in F_{q^d}, that is, the degree d extension field of F_q. We denote $F^* = F \setminus \{0\}$. Clearly, the multiplicative group F_q^* is a subgroup of the multiplicative group $F_{q^d}^*$.

By $[n, n-r]_q R$ we denote a q-ary linear code with length n, codimension r (and thus dimension $n-r$), and covering radius R. Given the parity check matrix $\mathbf{H}$ of a code with codimension r, the covering radius is the smallest integer R such that any vector in F_q^r can be expressed as a linear combination of at most R columns of $\mathbf{H}$. In this paper, we are

* This work was supported by the Academy of Finland

interested in the length function $l(r, R; q)$, that is—given r, R, and q—the smallest possible length n for an $[n, n-r]_q R$ code. For an introduction to covering codes, see [2].

In Section 2, generalizations of the construction in [1] are considered. In Section 3, the new codes are lengthened using methods from [3]. A table of upper bounds on $l(r, 2; q)$ for $r \leq 24$ and $q = 3, 5$ is given in Section 4.

2. Lengthening of BCH Codes

We shall first discuss some properties of the extension field F_{q^d}. We define

$$W = \frac{q^d - 1}{q - 1} = \sum_{i=0}^{d-1} q^i. \tag{1}$$

Since q^i is odd for all i, W is even if d is even and odd otherwise. The *norm* of elements of a field will turn out to be a very useful tool here. The norm of an element $\beta \in F_{q^d}$ over the field F_q is (see, for example, [7, Definition 2.27])

$$N_{F_{q^d}/F_q}(\beta) = \prod_{i=0}^{d-1} \beta^{q^i} = \beta^W. \tag{2}$$

For a proof of the following result, see [7, Theorem 2.28].

LEMMA 1 *$N_{F_{q^d}/F_q}(\beta) \in F_q$ and this function is surjective (onto).*

The concepts of quadratic residues (QRs) and quadratic nonresidues (QNRs) are important in finite fields with odd basis.

THEOREM 1 *For $k \geq 1$, all elements in F_q^* are QRs in the extension field $F_{q^{2k}}$.*

Proof. From (2), Lemma 1, and the fact that W is even (see comment after (1)), we get that for each $\gamma \in F_q^*$ there is a $\beta \in F_{q^{2k}}^*$ such that $\gamma = \beta^W = (\beta^{W/2})^2$, so γ is a QR. ■

A basic result in group theory is that since the multiplicative group F_q^* is a subgroup of the multiplicative group $F_{q^d}^*$, $F_{q^d}^*$ is partitioned by cosets of F_q^* (left and right cosets coincide as the groups are commutative).

THEOREM 2 *For $k \geq 1$, the elements of a coset of F_q^* in $F_{q^{2k}}^*$ are either all QNRs or all QRs.*

Proof. A coset of F_q^* is obtained as $gF_q^* = \{gf \mid f \in F_q^*\}$, $g \in F_{q^{2k}}^*$. As all elements in F_q^* are QRs (Theorem 1), then all elements in gF_q^* are QRs if g is a QR, and QNRs otherwise. ■

There are W cosets in total. Using this partitioning into cosets we can combinatorially prove a theorem corresponding to Theorem 1 for odd-degree extension fields.

THEOREM 3 *For $k \geq 0$, half of the elements in F_q^* are QRs (QNRs) in the extension field $F_{q^{2k+1}}$.*

Proof. Let there be a QRs and $(q-1-a)$ QNRs in F_q^* and let there be u cosets with a QRs and $W-u$ cosets with $(q-1-a)$ QRs. Then, as the total number of QRs in $F_{q^{2k+1}}$ is $W(q-1)/2$,

$$a(W-u)+(q-1-a)u = W(q-1)/2,$$

which gives

$$(2a-(q-1))(W-2u)=0,$$

so $a=(q-1)/2$ because W is odd and cannot be equal to $2u$. ■

Note that the cosets discussed correspond to points of the projective geometry PG$(d-1,q)$, and the parity check matrix of the $[W, W-d]_q 1$ Hamming code contains one element from each coset.

The codes constructed here and in [1] are lengthened BCH codes and have parity check matrices of size $(2d+1)\times n$ with the general form

$$\left[\begin{array}{ccccc|c} 1 & 1 & 1 & \cdots & 1 & \mathbf{0} \\ 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q^d-2} & \mathbf{0} \\ 0 & \alpha^0 & \alpha^2 & \cdots & \alpha^{q^d-3} & \mathbf{D} \end{array}\right], \qquad (3)$$

where the submatrix $\mathbf{D}$ is different in different constructions, $\alpha \in F_{q^d}$ is a primitive element, and each entry of the second and the third row is replaced by the corresponding column of d elements over F_q ($\mathbf{0}$ is a zero matrix of obvious size). The following theorem generalizes [1, Theorem 1]. Here the columns of $\mathbf{D}$ consist of one element from each coset of $F_{q^{2k}}^*$ with QNRs only.

THEOREM 4 *Let $q \geq 3$ be an odd prime power and $k \geq 1$. Then*

$$l(4k+1,2;q) \leq \frac{(2q-1)q^{2k}-1}{2(q-1)}.$$

Proof. We let $V=\{(1,\omega,\omega^2) \mid \omega \in F_{q^{2k}}\}$ and $V'=\{(0,0,\nu) \mid \nu \in S_N\}$, where S_N is any set with one element from each coset of $F_{q^{2k}}^*$ with QNRs only (so $|S_N| = W/2$, see Theorems 1 and 2). Then each vector $(a,b,c) \in F_q F_{q^{2k}} F_{q^{2k}}$ can be expressed in the following way as a linear combination with coefficients from F_q^* of at most two words in $V \cup V'$ (note that $-1, 1/2 \in F_q^*$):

$a=b=0$:	Follows from [1, Lemma 3];
$a=0, b\neq 0$:	$(1,u,u^2)-(1,v,v^2)$ with $u,v=(c\pm b^2)/2b$;
$a=1, c-b^2=0$:	$(1,b,b^2)$;
$a=1, c-b^2$ is a QR:	$(1,u,u^2)/2+(1,v,v^2)/2$ with $u,v=b\pm\sqrt{c-b^2}$;
$a=1, c-b^2$ is a QNR:	$(1,b,b^2)+w(0,0,v)$ with $wv=c-b^2$;
$a\neq 0,1$:	Follows from the cases with $a=1$ using $(a,b,c)=a(1,b/a,c/a)$.

By mapping the words in $V \cup V'$ to columns over F_q we get a parity check matrix for a q-ary covering code with covering radius 2. The total number of columns in this matrix is

$$n = q^{2k} + \frac{W}{2} \; = \; q^{2k} + \frac{q^{2k}-1}{2(q-1)} = \frac{(2q-1)q^{2k}-1}{2(q-1)}. \qquad \blacksquare$$

An important parameter that gives information about the quality of a (covering or error-correcting) code is the density. For a code with covering radius R, this gives the average number of codewords at distance less than or equal to R from any word in the space. Perfect codes have density 1. For a q-ary linear code of length n, codimension r and covering radius 2, the density is

$$\mu = \frac{1 + (q-1)n + (q-1)^2 n(n-1)/2}{q^r}. \tag{4}$$

For a given value of q, calculation of the density of a code constructed in Theorem 4 reveals that as k (and so n) tends to infinity, the density tends to

$$\frac{(2q-1)^2}{8q} = \frac{q-1}{2} + \frac{1}{8q} = \left\lfloor \frac{q}{2} \right\rfloor + \frac{1}{8q}. \tag{5}$$

In [1, Theorem 2], a similar construction to that of Theorem 4 is given (which works for $r = 4k+3$). A generalization of that construction is also possible (and the density of the codes tends to $q/2$ as r tends to infinity). However, it does not lead to any new bounds, so we do not consider it here. But for $q \geq 5$ we can obtain the following result. The proof partly mimics that of Theorem 4. Now the submatrix $\mathbf{D}$ in the parity check matrix (3) is taken to be the parity check matrix of an $[n', n' - (2k+1)]_q 2$ code.

THEOREM 5 *Let $q \geq 5$ be an odd prime power and $k \geq 0$. Then*

$$l(4k+3, 2; q) \leq q^{2k+1} + l(2k+1, 2; q).$$

Proof. We let $V = \{(1, \omega, \omega^2) \mid \omega \in F_{q^{2k+1}}\}$ and $V' = \{(0, 0, \nu) \mid \nu \in V''\}$, where V'' is the set of columns of a parity check matrix for an $[n', n' - (2k+1)]_q 2$ code. Now, a vector $(a, b, c) \in F_q F_{q^{2k+1}} F_{q^{2k+1}}$ can be expressed in the following way as a linear combination with coefficients from F_q^* of at most two words in $V \cup V'$ (note that $-1 \in F_q^*$):

$a = b = 0$:	Follows from the particular choice of V';
$a = 0, b \neq 0$:	$(1, u, u^2) - (1, v, v^2)$ with $u, v = (c \pm b^2)/2b$;
$a = 1, c - b^2 = 0$:	$(1, b, b^2)$;
$a = 1, c - b^2 \neq 0$:	$(1-t)(1, u, u^2) + t(1, v, v^2)$ with $v = b + \sqrt{\frac{1-t}{t}(c - b^2)}$, $u = (b - tv)/(1-t)$, where $t \in F_q^* \setminus \{1\}$ such that $(1-t)/t$ and $(c - b^2)$ are both QRs or both QNRs;
$a \neq 0, 1$:	Follows from the cases with $a = 1$ using $(a, b, c) = a(1, b/a, c/a)$.

In the fourth case, any of the two possible values of the square root may be used. The value of t has to be chosen based on whether $(c - b^2)$ is a QR or a QNR. For different $t \in F_q^* \setminus \{1\}$, we get different values of $(1 - t)/t$, which are all in F_q^*. Now, since half of the elements in F_q^* are QRs (and the other half are QNRs) in $F_{q^{2k+1}}$ (Theorem 3), a feasible value of t can always be found if $q \geq 5$ (but note that this is not possible if $q = 3$ since then there is only one possible value for t, as $|F_3^* \setminus \{1\}| = 1$).

By mapping the words in $V \cup V'$ to columns over F_q we get a parity check matrix for a q-ary covering code with covering radius 2. The length of the code is $q^{2k+1} + n'$, and as we can make $n' = l(2k+1, 2; q)$, we get that $l(4k+3, 2; q) \leq q^{2k+1} + l(2k+1, 2; q)$.

■

Since Theorem 5 is recursive, calculation of the density of the code families is not straightforward. From Theorems 4 and 5 we get that $0 < l(2k+1, 2; q) < 2q^k$ (the bounds are rough but sufficient). Now calculating the densitity (4) using the lower and upper bounds, q^{2k+1} and $q^{2k+1} + 2q^k$, on the lengths of the codes constructed in Theorem 5 in both cases leads to the following asymptotic value of the density as k (and n) tends to infinity:

$$\frac{q}{2} - 1 + \frac{1}{2q}. \tag{6}$$

Interestingly, a slight modification of Theorem 5 gives a recursive construction of complete caps in projective spaces [6].

In the last construction of this section, we use the parity check matrix

$$\left[\begin{array}{ccccc|ccccc|c} 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 1 & \cdots & 1 & \mathbf{0} \\ 1 & 1 & 1 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 & \mathbf{0} \\ 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q^d-2} & 0 & 0 & 0 & \cdots & 0 & \mathbf{H}_d \\ 0 & \alpha^0 & \alpha^2 & \cdots & \alpha^{q^d-3} & 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{q^d-2} & \mathbf{0} \end{array}\right] \tag{7}$$

with even codimension $2 + 2d$, where $\mathbf{H}_d$ is the parity check matrix of the $[n_d = (q^d - 1)/(q - 1), n_d - d]_q 1$ Hamming code.

THEOREM 6 *Let $q \geq 5$ be an odd prime power and $k \geq 1$. Then*

$$l(4k, 2; q) \leq 2q^{2k-1} + \frac{q^{2k-1} - 1}{q - 1}.$$

Proof. For $d = 2k - 1$, we want to show that any vector $(a, b, c, e) \in F_q F_q F_{q^{2k-1}} F_{q^{2k-1}}$ can be expressed as a linear combination with coefficients from F_q^* of at most two columns of (7). This can be done in the following ways:

$a = 0$: Use the first q^{2k-1} columns of (7) as shown in the proof of Theorem 5, except for the case $b = 0$, $c = 0$, when $(0, 0, 0, e) = (1, 0, 0, e) - (1, 0, 0, 0)$;

$a = 1, b = 0$: $(1, 0, 0, e) + u(0, 0, c/u, 0)$, where c/u is a column vector of $\mathbf{H}_{2k-1}$;

$a = 1, b \neq 0$: $b(0, 1, c/b, (c/b)^2) + (1, 0, 0, e - c^2/b)$;

$a \neq 0, 1$: Follows from the cases with $a = 1$ using $(a, b, c, e) = a(1, b/a, c/a, e/a)$.

Hence the covering radius is 2. The length and the codimension of the code over F_q are obvious, so the proof is completed. ■

For $k = 1$, Theorem 6 gives $l(4, 2; q) \leq 2q + 1$, which coincides with the result in [3, Theorem 5.1] for odd q. For $k = 2$, we get $l(8, 2; q) \leq 2q^3 + q^2 + q + 1$, whereas the upper bound given in [4] and [5] is $2q^3 + q^2 + 2q + 2$. The density of the codes from Theorem 6 tends to

$$2 - \frac{2}{q} + \frac{1}{2q^2}$$

as k (and n) tends to infinity.

3. A q^m-Concatenating Construction

In [1], the authors conjectured that a construction from [3] could be applied to find further improvements for ternary covering codes using the new codes. Here we shall see that this is indeed the case. Constructions from [3] will successfully be applied to the codes obtained here and in [1]. These constructions were termed *q^m-concatenating* in [4], [5].

Let $\mathbf{H}' = [h'_1\ h'_2\ \cdots\ h'_{n'}]$ be the parity check matrix of an $[n', n' - r]_q 2$ starting code. The parity check matrix for the codes obtained in the q^m-concatenating construction here has the following general form:

$$\mathbf{H} = \left[\begin{array}{cccc|c|cccc|c} h'_1 & h'_1 & \cdots & h'_1 & \cdots & h'_{n'} & h'_{n'} & \cdots & h'_{n'} & \\ 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \cdots & 0 & \alpha^0 & \cdots & \alpha^{q^m-2} & \mathbf{A} \\ 0 & \beta_1\alpha^0 & \cdots & \beta_1\alpha^{q^m-2} & \cdots & 0 & \beta_{n'}\alpha^0 & \cdots & \beta_{n'}\alpha^{q^m-2} & \end{array}\right], \tag{8}$$

where α is a generator of F_{q^m} and $\beta_i \in F_{q^m}$ with some further restrictions. We further denote $\mathbf{H} = [h_1\ h_2\ \cdots\ h_n]$. The matrix $\mathbf{A}$ of size $(r + 2m) \times n''$ varies in different variants of this construction and the new code will be an $[n = n'q^m + n'', n - (2m + r)]_q 2$ code when the parameters are chosen carefully.

In the basic version of the construction, we let

$$\mathbf{A} = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{H}_m & \mathbf{0} \\ \mathbf{0} & \mathbf{H}_m \end{bmatrix} \tag{9}$$

and require that $\beta_i \neq \beta_j$ when $i \neq j$. This is a variant of Construction A32$_2$ in [3, Notation 6.1].

THEOREM 7 *Let $q \geq 2$ be a prime power and $q^m \geq l(r, 2; q)$. Then*

$$l(r + 2m, 2; q) \leq q^m l(r, 2; q) + \frac{2(q^m - 1)}{q - 1}.$$

Proof. We prove that the code with parity check matrix from (8) and (9) has covering radius 2. Since the code with parity check matrix $\mathbf{H}'$ has covering radius 2, every element

$a \in F_{q^r}$ can be written as $a = sh'_i + th'_j$ with $i \neq j$ and $s, t \in F_q$. When we want to solve the equation $sh_k + th_l = x$, with $x = (a, b, c) \in F_{q^r} F_{q^m} F_{q^m}$, we get three subcases depending on whether s and t are zero or nonzero:

Case 1: $s = t = 0$: $(a = 0)$ Now we can write $(0, b, c) = (0, b, 0) + (0, 0, c) = u(0, b/u, 0) + v(0, 0, c/v)$, where b/u and c/v are column vectors of $\mathbf{H}_m$.

Case 2: $s \neq 0, t = 0$: Here $a = sh'_i$ and we get that $(a, b, c) = s(h'_i, b/s, \beta_i(b/s)) + u(0, 0, (c - \beta_i b)/u)$, where $(c - \beta_i b)/u$ is a column vector of $\mathbf{H}_m$.

Case 3: $s \neq 0, t \neq 0$: In this final case, when $a = sh'_i + th'_j$, we end up with the equation system

$$\left\{ \begin{array}{r} su + tv = b \\ s\beta_i u + t\beta_j v = c \end{array} \right.$$

which we want to solve for $u, v \in F_{q^m}$. Since the determinant of this equation system is $st(\beta_j - \beta_i) \neq 0$, there is a solution (remember that $\beta_i \neq \beta_j$ when $i \neq j$).

The proof is now completed. To minimize the length n we use a starting code of length $l(r, 2; q)$. ■

Actually, by slightly altering the parity check matrix, $q^m \geq l(r, 2; q)$ could be replaced by $q^m + 1 \geq l(r, 2; q)$ in Theorem 7 (see [3, Condition A3]). However, this would not affect the results in this paper.

In the second q^m-concatenating construction used here (which is Construction C12$_1$ in [3]), we let

$$\mathbf{A} = \begin{bmatrix} \mathbf{0} \\ \mathbf{0} \\ \mathbf{H}_m \end{bmatrix}. \tag{10}$$

Since this matrix has fewer columns than (9), we need further requirements on β_i. In fact, we want

$$\{\beta_1, \beta_2, \ldots, \beta_{n'}\} = F_{q^m}. \tag{11}$$

We must then have $n' \geq q^m$, and since $n' = q^m$ would be very restrictive, we would like to allow some of the values of β_i to be the same. This is indeed possible under the following conditions.

We partition the set $\{1, 2, \ldots, n'\} = S_0 \cup S_1 \cup \cdots \cup S_{q^m-1}$ such that all elements in F_{q^r} which are not obtainable as the multiple of one column of $\mathbf{H}'$ can be obtained as $sh'_i + th'_j$, where i and j belong to different subsets of the partition. If this is possible we say that the code has a q^m-partition. We define a one-to-one correspondence between the sets S_i and the elements in F_{q^m}. In the construction, if $i \in S_a$ we let β_i take the corresponding value in F_{q^m}.

THEOREM 8 *Let $q \geq 2$ be a prime power. If there is an $[n', n' - r]_q 2$ code C, $q^m \leq n'$, and C has a q^m-partition, then*

$$l(r + 2m, 2; q) \leq q^m n' + \frac{q^m - 1}{q - 1}.$$

Proof. We consider the code C with parity check matrix from (8) and (10), and assume that $q^m \leq n'$ and that C has a q^m-partition. We shall show that C has covering radius 2. We know that every element $a \in F_{q^r}$ can be written as $a = sh'_i + th'_j$ with $i \neq j$ and $s, t \in F_q$ with i and j belonging to different subsets of the q^m-partition. When we want to solve $sh_k + th_l = x$, with $x = (a, b, c) \in F_{q^r} F_{q^m} F_{q^m}$, we get three subcases:
Case 1: $s = t = 0$: $(a = 0)$ If $b = 0$, then we have a solution using one column from (10). If $b \neq 0$, then we take $(0, b, c) = (h'_p, b, \beta_p b) - (h'_p, 0, 0)$, where $\beta_p = c/b$. Such a p exists because of (11).
Case 2: $s \neq 0, t = 0$: Coincides with the proof of Theorem 7.
Case 3: $s \neq 0, t \neq 0$: Coincides with the proof of Theorem 7 after noticing that due to the q^m-partition, $\beta_i \neq \beta_j$. ■

Note that, compared to Theorem 7, we now use n' and not $l(r, 2; q)$ in the statement since—for given values of q, r, and m—occasionally Theorem 8 can only be applied to codes of some length $n' > l(r, 2; q)$ (this is clearly always the case if $l(r, 2; q) < q^m$).

Applying the q^m-concatenating construction to the new code families gives several code families, which will be presented in the following theorems. We define the parity function $p(x) \equiv x \pmod 2$, $p(x) \in \{0, 1\}$.

THEOREM 9 *Let $q \geq 3$ be an odd prime power and $k \geq 2$. Then*

$$l(4k + 3, 2; q) \leq \frac{(2q - 1)q^{2k+1} + 3q^{k+1+p(k)} - 4}{2(q - 1)}.$$

Proof. From Theorem 4, we have that for $k' \geq 1$, $l(4k' + 1, 2; q) \leq \frac{(2q-1)q^{2k'}-1}{2(q-1)}$. Since $q^{2k'} < \frac{(2q-1)q^{2k'}-1}{2(q-1)} < q^{2k'+1}$, Theorem 7 can be applied when $m \geq 2k'+1$; we shall consider $m = 2k' + 1$ and $m = 2k' + 3$. In these two cases we get (after substituting $k = 2k'$ and $k = 2k' + 1$, respectively) that when $k \geq 2$ is even,

$$l(4k + 3, 2; q) \leq \frac{(2q - 1)q^{2k+1} + 3q^{k+1} - 4}{2(q - 1)}$$

and when $k \geq 3$ is odd,

$$l(4k + 3, 2; q) \leq \frac{(2q - 1)q^{2k+1} + 3q^{k+2} - 4}{2(q - 1)},$$

which can be unified to get the desired result. ■

Calculation reveals that the asymptotic density as n tends to infinity of the codes from Theorem 9 (with $r = 4k + 3$) coincides with that of the starting codes (with $r = 4k + 1$), given in (5). (But the density of a new code is slightly greater than that of the starting code.) For $q = 3$ and $r = 4k + 3$, the asymptotic density for the codes obtained in [4] is approximately 1.178 whereas it is $25/24 \approx 1.042$ here.

The codes from Theorem 5 can also be used as starting codes, and we can in fact use the construction in Theorem 8.

THEOREM 10 *Let $q \geq 5$ be an odd prime power and $k \geq 1$. Then*

$$l(4k+1,2;q) \leq q^{2k} + l(k-1+p(k),2;q)q^{k+1-p(k)} + (2-p(k))\frac{q^{k+1-p(k)}-1}{q-1}.$$

Proof. From Theorem 5, we have that for $k' \geq 0, l(4k'+3,2;q) \leq q^{2k'+1}+l(2k'+1,2;q)$. From the proof of Theorem 5, it is clear that the code obtained has a $q^{2k'+1}$-partition (in each subset, take one column from V and at most one column from V'). We can then apply Theorem 8 with $m = 2k'+1$ and we get that when $k \geq 1$ is odd,

$$l(4k+1,2;q) \leq q^{2k} + l(k,2;q)q^k + \frac{q^k-1}{q-1}.$$

By further applying Theorem 7 with $m = 2k'+3$ we get that when $k \geq 2$ is even,

$$l(4k+1,2;q) \ \leq \ q^{2k} + l(k-1,2;q)q^{k+1} + \frac{2(q^{k+1}-1)}{q-1}. \qquad \blacksquare$$

Again, the asymptotic density of the new codes (with $r = 4k+1$) coincides with that of the starting codes (with $r = 4k+3$) given in (6). In the calculation of the density, we need bounds for $l(r,2;q)$; cf. remark after Theorem 5. We can here use, for example, $0 < l(r,2;q) < 2q^{r/2}$, which follows from $l(2k+1,2;q) \leq 2q^k$ used earlier and the bound $l(2k+2,2;q) \leq 2q^{k+1}$ derived using $l(k+1,2;q) \leq ql(k,2;q)$. It turns out that for the density calculations, the only significant term on the right side of the inequality in Theorem 10 is q^{2k}. For example, for $q = 5$ with $r = 2k+1$, the density is 1.6 compared to 2.304 for the family constructed in [4].

THEOREM 11 *Let $k \geq 3$. Then*

$$l(4k,2;3) \leq \frac{5 \cdot 9^k + 3^{k+2-p(k)}}{6} - 1.$$

Proof. We now start from codes obtained by applying $l(r+1,2;3) \leq 2l(r,2;3)$ [4], [8] to the codes from [1, Theorem 1] (or, from Theorem 4 with $q = 3$). For such codes $l(4k'+2,2;3) \leq (5 \cdot 9^{k'} - 1)/2$, $k' \geq 1$. By using Theorem 7 with $m = 2k'+1$ and $m = 2k'+3$, respectively, and combining the results, the theorem is proved similarly to Theorem 9. $\blacksquare$

The density of the codes from Theorem 11 (as well as that of the starting codes) tends to $25/18 \approx 1.389$ as k (and n) tends to infinity (cf. [1]). This improves on the asymptotic density obtained in [4], which is approximately 1.447. Note that we can also try to apply $l(r+1,2;3) \leq 2l(r,2;3)$ to Theorem 9 to get bounds for the same parameters, but the results will turn out to be slightly worse than by using Theorem 11 (the asymptotic density is the same).

Table 1. Upper bounds on $l(r, 2; q)$ for $r \leq 24$, $q = 3, 5$.

r	$l(r, 2; 3)$	$l(r, 2; 5)$	r	$l(r, 2; 3)$	$l(r, 2; 5)$
3	4^i	6^i	14	1822^h	35000^k
4	8^h	11^c	15	2915^d	78256^b
5	11^a	28^a	16	5588^f	175000^k
6	22^h	56^k	17	8201^a	410937^e
7	40^g	131^b	18	16402^h	875000^k
8	76^j	281^c	19	24785^d	1953828^b
9	101^a	703^a	20	49328^f	4375000^k
10	202^h	1400^k	21	73811^a	9853906^e
11	323^d	3153^b	22	147622^h	21875000^k
12	620^f	7031^c	23	223073^d	48831278^b
13	911^a	16406^e	24	443960^f	109375000^k

Key to Table 1.
a—Theorem 4 (also [1, Theorem 1] for $q = 3$)
b—Theorem 5
c—Theorem 6
d—Theorem 9
e—Theorem 10
f—Theorem 11
g—[1, Theorem 2]
h—$l(r + 1, 2; 3) \leq 2l(r, 2; 3)$ [4], [8]
i—See [9, Table I]
j—[3]
k—[5]

4. A New Table

We conclude the paper by presenting upper bounds on $l(r, R; q)$ for $r \leq 24$, $R = 2$, and $q = 3, 5$ in Table 1. For recent tables of linear q-ary codes with these parameters, see [1], [4], [5]. The bounds $l(11, 2; 3) \leq 323$ and $l(15, 2; 3) \leq 2915$ and $l(4, 2; 5) \leq 11$ were also obtained in [3], the bounds $l(12, 2; 3) \leq 620$ and $l(16, 2; 3) \leq 5588$ in [4], and the bound $l(12, 2; 5) \leq 7031$ in [5].

Acknowledgment

This work was carried out while the first author was visiting Helsinki University of Technology. He gratefully acknowledges the Academy of Finland and Helsinki University of Technology for hospitality during this visit.

References

1. J. C. Cock and P. R. J. Östergård, Ternary covering codes derived from BCH codes, *J. Combin. Theory. Ser. A*, Vol. 80 (1997) pp. 283–289.

2. G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland Mathematical Library, Vol. 54, Elsevier, Amsterdam (1997).
3. A. A. Davydov, Constructions and families of covering codes and saturated sets of points in projective geometry, *IEEE Trans. Inform. Theory*, Vol. 41 (1995) pp. 2071–2080.
4. A. A. Davydov, On nonbinary linear codes with covering radius two, Proceedings of the Fifth International Workshop on Algebraic and Combinatorial Coding Theory, Unicorn, Shumen, Bulgaria (1996) pp. 105–110.
5. A. A. Davydov, Constructions and families of nonbinary linear codes with covering radius 2, submitted.
6. A. A. Davydov and P. R. J. Östergård, Recursive constructions of complete caps, submitted.
7. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley, Reading, MA (1983).
8. P. R. J. Östergård, New constructions for q-ary covering codes, *Ars Combin.*, to appear.
9. F. Pambianco and L. Storme, Small complete caps in spaces of even characteristic, *J. Combin. Theory. Ser. A*, Vol. 75 (1996) pp. 70–84.