New Constructions for q-ary Covering Codes

Patric R. J. Östergård*
Department of Mathematics and Computing Science
Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands

Abstract

Upper bounds on $K_q(n, R)$, the minimum number of codewords in a q-ary code of length n and covering radius R, are improved. Such bounds are obtained by constructing corresponding covering codes. In particular, codes of length $q + 1$ are discussed. Good such codes can be obtained from maximum distance separable (MDS) codes. Furthermore, they can often be combined effectively with other covering codes to obtain new ones. Most of the new codes are obtained by computer search using simulated annealing. The new results are collected in updated tables of upper bounds on $K_q(n, R)$, $q = 3, 4, 5$.

1. Introduction

We consider codes $C \subseteq F_q^n$, where F_q^n is the set of all words of length n over F_q. If q is a prime power, we let F_q be the Galois field $GF(q)$, otherwise F_q is the set of integers modulo q. The Hamming distance $d(x, y)$ between two words $x, y \in F_q^n$ is the number of coordinates where they differ. The *covering radius* of a code C is the smallest integer R with the property that for each $x \in F_q^n$ there is a codeword $c \in C$ such that $d(x, c) \leq R$. A code $C \subseteq F_q^n$ that has covering radius R is said to be a $(q, n, |C|)R$ code. If the code is a linear code with length n and q^k codewords, we use the notation $[n, k]_q R$ (notations $(q, n, |C|)$ and $[n, k]_q$ are used if the value of R is insignificant). The main interest in the study of nonlinear covering codes is determination of values of the following function:

$$K_q(n, R) = \min\{M \mid \text{there is a } (q, n, M)R \text{ code}\}.$$

*The research was supported by the Academy of Finland.

In [5] and [16], extensive tables of lower and upper bounds, respectively, for 3-ary, 4-ary, and 5-ary covering codes are presented. In this paper new tables of best known upper bounds are given, thus updating the tables in [16]. Lower bounds are not given; however, known exact values are indicated in the tables.

In Section 2 good codes of length $q+1$ obtained from maximum distance separable (MDS) codes are discussed. Many such codes are also shown to have a partitioning property, which makes them important building blocks in constructions of new covering codes from old ones. A matrix method is presented in Section 3. The method has earlier been used with success to produce good binary, ternary, and mixed covering codes. Many of the new bounds in this paper are obtained by computer search using this method and a heuristic called simulated annealing. An improvement of a lengthening construction by Honkala is discussed in Section 4; this construction is used to obtain new linear covering codes. Finally, in Section 5, upper bounds for the following functions are given: $K_3(n,R)$ for $1 \leq n \leq 14$, $1 \leq R \leq 9$; $K_4(n,R)$ for $1 \leq n \leq 10$, $1 \leq R \leq 7$; and $K_5(n,R)$ for $1 \leq n \leq 9$, $1 \leq R \leq 7$. New codes obtained by the matrix method are listed in the Appendix.

2. Covering Codes from MDS Codes

A q-ary *maximum distance separable* (MDS) code with q^k codewords has the property that for any k coordinates, each of the q^k possible k-tuples occurs in exactly one codeword. If the length of the code is n, then the minimum distance is $d = n - k + 1$ [22]. It is easily seen that no code with the same length and number of codewords can have greater minimum distance; this explains the name of this class of codes. It is known that if q is a prime power, then $[q+1,k]_q$ MDS codes exist for all $1 \leq k \leq q+1$ [15, Ch. 11, Theorem 9]. Shortening these codes we get that MDS codes exist for all $1 \leq k \leq n$, $1 \leq n \leq q+1$. MDS codes lead to good covering codes of length $q+1$ as the following theorem shows.

Theorem 1 *If q is a prime power and no linear $[q+2, q-R+1]_q$ MDS code exists, then $K_q(q+1,R) \leq q^{q-R}$.*

Proof: The minimum distance of a $[q+1, q-R]_q$ MDS code is $R+2$. For every $x \in F_q^n$ and each set of $k = q-R$ coordinates, there is a codeword that coincides in these coordinates; the covering radius is thus at most $(q+1)-(q-R) = R+1$. If the covering radius is $R+1$, then a column can be added to the parity check matrix of the code without decreasing the minimum distance; this, however, is not possible as we assume that there exists no $[q+2, q-R+1]_q$ MDS code. Hence the covering radius is at most

R and the code shows that $K_q(q+1,R) \leq q^{q-R}$. □

Unfortunately, Theorem 1 cannot always be applied, since $[q+2,k]_q$ codes are known to exist for q even and dimensions $k=3$ and $k=q-1$. (No other parameters for which $[q+2,k]_q$ codes exist are known; moreover, for $q \leq 11$ it has been proved that these are the only parameters for which such codes exist [15, p. 328].) The next theorem is able to fill such gaps; furthermore, it gives coverings when q is not a prime power.

Theorem 2 *If there exists a* $(q, q-R+2, q^{q-R})$ *MDS code where* $1 \leq R \leq q-1$, *then* $K_q(q+1,R) \leq q^{q-R}$.

Proof: For $1 \leq R \leq q-1$, let C be a q-ary MDS code with q^{q-R} codewords and length $q-R+2$, and let $C_i = \{x \mid (i,x) \in C\}$.

We first show that for every $x \in F_q^{q-R+1}$, either there is an i such that $d(x,C_i)=0$; or $d(x,C_i)=1$ for $q-R+1$ different subcodes C_i. Take any $q-R$ of the coordinates of x (this can be done in $q-R+1$ ways). For all these choices, there is a codeword that meets exactly in these coordinates. Now assume that for two of the choices, the codewords, say c_1 and c_2, belong to the same set C_i. However, then $d(c_1,c_2) \leq 2$, so $c_1 = c_2$ due to the MDS property of the original code C; in this case $d(x,C_i)=0$. Also, for all i, $d(x,C_i) \leq 2$ due to the MDS property of C.

Now consider the code $C' = \bigcup_i (i,i,\ldots(R \text{ times})) \oplus C_i$. Take any $(x,y) \in F_q^{q+1}$, where $x \in F_q^R$ and $y \in F_q^{q-R+1}$. If there is an i such that $d(y,C_i)=0$, then $d((x,y),C') \leq R$. Otherwise, if at least two of the coordinates of x have the same values, then $d(x,C') \leq (R-2)+2 = R$. Finally we have to consider the case when $d(x,(i,i,\ldots)) = R-1$ for R values of i, and $d(y,C_i)=1$ for $q-R+1$ values of i. Then, since $R+(q-R+1) = q+1 > q$, we get that $d((x,y),C') = (R-1)+1 = R$. This completes the proof. □

Note that the codes obtained in Theorem 2 are not MDS for $R>1$. Using known MDS codes in Theorem 2, we obtain a corollary slightly stronger than Theorem 1.

Corollary 1 *If* q *is a prime power, then* $K_q(q+1,R) \leq q^{q-R}$ *for* $1 \leq R \leq q-1$.

Actually, we have equality in Corollary 1 for $R=1$, q a prime power (Hamming codes), and in Theorems 1 and 2 and Corollary 1 for $R=q-1$ [5]. Corollary 1 reproves the bounds $K_4(5,2) \leq 16$, $K_5(6,2) \leq 125$, and $K_5(6,3) \leq 25$ given in [16]. As for the last two of these bounds, generator matrices of corresponding linear codes were given in [16]; the first bound was proved by explicitly listing the codewords.

For $k = 2$, there is a (q, n, q^2) MDS code exactly when there are $(n-2)$ mutually orthogonal Latin squares of order q [7, Theorem 3], [22, Theorem 3]. Since 2 mutually orthogonal Latin squares exist whenever $q \neq 2, 6$ [2], we get the following result, which is not restricted to codes over prime power alphabets.

Corollary 2 *$K_q(q+1, q-2) \leq q^2$ for all $q \neq 2, 6$.*

If we restrict our discussion to linear codes over $GF(q)$, codes with the same parameters as ours are equivalent to $(R-1)$-saturated (or R-spanning) sets with $n = q+1$ points in the projective geometry $PG(R, q)$. The problem of finding the minimum n for which such sets exist has recently been studied in several papers; for references and a short summary of results, see [6]. For large q and $R = 2$ it is possible to find $(R-1)$-saturated sets in $PG(R, q)$ with less than $q+1$ points. For example, for $q \geq 8$ and $R = 2$, there are such sets with $\lfloor q/2 + 2 \rfloor$ points.

We shall now show that there are $(q, q+1, q^{q-R})R$ codes that can be used as building blocks in constructing new codes. A $(q, n, M)R$ code is *strongly k-seminormal* if it can be partitioned into k subcodes that all have covering radius $R+1$ [16] (the term *strongly seminormal* is used if $k = q$).

Theorem 3 *If there exists a $(q, q-R+3, q^{q-R})$ MDS code where $2 \leq R \leq q-2$ and $q-R$ is even, then there is a strongly seminormal $(q, q+1, q^{q-R})R$ code.*

Proof: Let C be a q-ary MDS code with q^{q-R} codewords and length $q-R+3$ and let $C_i = \{x \mid (i, x) \in C\}$. Now, deleting the last coordinate of the code $C'' = \bigcup_i (i, i, \ldots (R \text{ times})) \oplus C_i$, we get a $(q, q+1, q^{q-R})R$ code C' as in the proof of Theorem 2. We shall now prove that the partition $C' = \bigcup_i C'_i$, where $C'_i = \{x \mid (x, i) \in C''\}$, proves strong seminormality of C'. W.l.o.g, we show that $C''' = \bigcup_i (i, i, \ldots (R \text{ times})) \oplus C'''_i$, where $C'''_i = \{x | (i, x, 0) \in C\}$, has covering radius $R+1$.

The following is a slight modification of the corresponding steps in the proof of Theorem 2. We first show that for every $x \in F_q^{q-R+1}$, either there is an i, such that $d(x, C'''_i) \leq 1$; or $d(x, C'''_i) \leq 2$ for at least $q-R+1$ different subcodes C'''_i. Take any $q-R-1$ of the coordinates of x; this can be done in $(q-R+1)(q-R)/2$ ways. For all these choices, there is a codeword in $\bigcup_i C'''_i$ that meets exactly in these coordinates. If there is a subcode C'''_i to which at least $\lceil (q-R+1)/2 \rceil$ of these codewords belong, then there are two codewords, say c_1 and c_2, with the property that $d(c_1, c_2) \leq 2$, so $c_1 = c_2$ due to the MDS property of C; thus $d(x, C'''_i) \leq 1$. On the other hand, if all subcodes C'''_i contain at most $\lfloor (q-R+1)/2 \rfloor$ of these codewords, then the codewords belong to at least $((q-R+1)(q-R)/2)/\lfloor (q-R+1)/2 \rfloor = q-R+1$ different subcodes C'''_i; for these subcodes, $d(x, C'''_i) \leq 2$ ($\lfloor (q-R+1)/2 \rfloor =$

$(q-R)/2$ when $q-R$ is even). Also, for all i, $d(x, C_i''') \leq 3$ due to the MDS property of C.

Now take any $(x, y) \in F_q^{q+1}$, where $x \in F_q^R$ and $y \in F_q^{q-R+1}$. If there is an i such that $d(y, C_i''') \leq 1$, then $d((x, y), C''') \leq R+1$. Otherwise, if at least two of the coordinates of x have the same values, then $d((x, y), C''') \leq (R-2)+3 = R+1$. Finally we have to consider the case when $d(x, (i, i, \ldots)) = R-1$ for R values of i, and $d(y, C_i''') \leq 2$ for at least $q-R+1$ values of i. Then, since $R+(q-R+1) = q+1 > q$, we get that $d((x, y), C''') \leq (R-1)+2 = R+1$, which completes the proof. □

These codes can be used in constructions of new codes from old ones. If q is a prime power, we now get the following very useful result by applying [16, Theorem 4] to a $(q, n, K_q(n, R))R$ code and a strongly seminormal $(q, q+1, q^{q-R'})R'$ code.

Corollary 3 *If q is a prime power, $2 \leq R' \leq q-2$, and $q-R'$ is even, then $K_q(n+q, R+R') \leq q^{q-R'-1} K_q(n, R)$, where the code corresponding to $K_q(n, R)$ must have a coordinate where all q values occur.*

Codes proving $K_q(q+1-p, R) \leq q^{q-R-p}$ $(p > 0)$ discussed earlier can be used to get better constructions for large q. Namely, if C is such a code, then $C \oplus \{0, 1, \ldots q-1\}$ is strongly seminormal and we get a construction giving $K_q(n+q-p+1, R+R') \leq q^{q-R'-p} K_q(n, R)$.

The result in Corollary 3 is similar to that in [16, Theorem 3]. Note that the $[q+1, q-R]_q R$ MDS codes in Theorem 1 are not strongly seminormal as they have minimum distance $R+2$, which then is the smallest possible covering radius for the subcodes in a partitioning. However, partitions of such codes can still be useful in constructions if we require additional properties of the codes we act upon. For partitioning constructions involving Hamming codes, see [9, 16, 17].

Although we have not been able to give a proof in the case $q-R'$ odd, it seems that Theorem 3 also holds for these parameters. As we later tabulate bounds on $K_q(n, R)$ for $q = 3, 4, 5$, the question whether a strongly seminormal $(5, 6, 125)2$ code exists is of particular interest. By construction we give an affirmative answer to that question.

Theorem 4 *There is a strongly seminormal $(5, 6, 125)2$ code. Thus $K_5(n+5, R+2) \leq 25 K_5(n, R)$.*

Proof: Consider the $(5, 6, 125)2$ MDS code C obtained from the following parity check matrix (from [15, p. 323]).

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 0 & 0 \\ 1 & 4 & 4 & 1 & 0 & 1 \end{bmatrix}.$$

Applying the construction in the proof of Theorem 3 to C, we obtain a code that is strongly seminormal. □

The $(3, 7, 12)3$ code given in [16] was proved to be strongly seminormal in that paper. It is even strongly 4-seminormal, which is proved by forming a fourth subset out of the last codewords in each of the subsets given in [16]. To make use of this property in the construction of good ternary codes we need good ternary/quaternary mixed codes. Mixed codes (mainly binary/ternary) have earlier been considered, for example, in [8, 14, 18, 21, 23]. Following the notations in [18, 21], we let $K_{q_1,q_2,\ldots,q_m}(n_1, n_2, \ldots, n_m; R)$ denote the minimum number of codewords in a code $C \subseteq F_{q_1}^{n_1} F_{q_2}^{n_2} \cdots F_{q_m}^{n_m}$ that has covering radius R. By applying [16, Theorem 4] to the strongly 4-seminormal $(3, 7, 12)3$ code, we get the following theorem.

Theorem 5 $K_3(n+7, R+3) \leq 3K_{4,3}(1, n; R)$.

From [21] we know that $K_{4,3}(1, 6; 2) \leq 36$; this gives a new bound in Table I, $K_3(13, 5) \leq 108$. Another improvement, $K_3(13, 6) \leq 45$, can be obtained from $K_{4,3}(1, 6; 3) \leq 15$ proved by the following code: Take the words in $C = \{0021210, 1000020, 1120020, 2212100, 3100210\} \subseteq F_4^1 F_3^6$ together with the words in $C + 0111111$ and $C + 0222222$. This code was actually found using the method to be presented in the next section (modified to work for mixed codes, cf. [18]).

3. A Matrix Method

In 1970, Kamps and Van Lint [11] gave a nice combinatorial proof of $K_3(9, 1) \leq 1458$. The method used in the proof was later further developed and generalized by Blokhuis and Lam [1] and Van Lint Jr. [13]. Let $\mathbf{A} = (\mathbf{I}; \mathbf{M}) = (a_1, \ldots, a_n)$ be an $r \times n$ matrix where $\mathbf{I}$ is the $r \times r$ identity matrix and $\mathbf{M}$ is an $r \times (n-r)$ matrix with entries from F_q. For a column vector $s \in F_q^r$, we define

$$S_{A,R}(s) = \{s + \sum_{j=1}^{R} \alpha_j a_{i_j} \mid \alpha_j \in F_q\}$$

for any R-subset $\{a_{i_1}, \ldots, a_{i_R}\}$ of $\{a_1, \ldots, a_n\}$, and say that s *R-covers* $S_{A,R}(s)$ *using* $\mathbf{A}$. If $\mathbf{A} = \mathbf{I}$, this covering coincides with covering in the traditional sense. More generally, a subset S of F_q^r is said to *R-cover* F_q^r *using* $\mathbf{A}$ if

$$F_q^r = \bigcup_{s \in S} S_{A,R}(s).$$

Theorem 6 (Van Lint Jr. [13, Theorem 1.4.4]). *If S R-covers F_q^r using an $r \times n$ matrix $\mathbf{A} = (\mathbf{I}; \mathbf{M})$, then $W = \{w \in F_q^n \mid \mathbf{A}w \in S\}$ covers F_q^n with radius R. $|W| = |S|q^{n-r}$.*

This method was used in this research to obtain new 3-ary, 4-ary and 5-ary covering codes. The codes together with the matrix $\mathbf{M}$ are listed in the Appendix; a new binary code proving $K_2(14, 1) \leq 1408$ is also included in the list. In the search for these codes, a search heuristic called simulated annealing has played a central role. The same approach as in [19] has been used; see that paper for further details. A code obtained by the matrix method is the union of some of the cosets of a linear code. Two of the new codes—a $(3, 14, 3^5)5$ code and a $(3, 14, 3^4)6$ code—are actually linear. These were found by checking linear codes with large minimum distance. A $(3, 14, 3^5)5$ code was earlier constructed by Kennedy [12].

4. An Improved Lengthening Construction

The matrix method presented in Section 3 can be used in constructing new codes from old. It has been shown [1, 13] that if C is a $(q, n, M)R$ code (q is a prime power), then $\{0\} \oplus C$ R-covers F_q^{n+1} using the following $(n+1) \times (qn+1)$ matrix:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & 1 & \cdots & 1 & 2 & \cdots & 2 & \cdots & q-1 & \cdots & q-1 \\ 0 & & & & & & & & & & & & & \\ \vdots & & I_n & & & I_n & & & I_n & & \cdots & & I_n & \\ 0 & & & & & & & & & & & & & \end{bmatrix}.$$

By using Theorem 6 we get that if q is a prime power, then $K_q(qn+1, R) \leq q^{n(q-1)} K_q(n, R)$. Although this construction works for $R \geq 1$, it gives record-breaking codes only for $R = 1$. For example, $K_2(14, 1) \leq 1408$ proved here gives a series of new bounds, starting with $K_2(29, 1) \leq 23068672$. Honkala [10], however, recognized that the construction can be improved under certain conditions. He shows that if q is a prime, then $N \oplus C$ R-covers F_q^{n+1} using the following $(n+1) \times (tn+1)$ matrix $\mathbf{A}$:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 & a_2 & \cdots & a_2 & a_3 & \cdots & a_3 & \cdots & a_t & \cdots & a_t \\ 0 & & & & & & & & & & & & & \\ \vdots & & I_n & & & I_n & & & I_n & & \cdots & & I_n & \\ 0 & & & & & & & & & & & & & \end{bmatrix},$$

where $N \subseteq F_q$ ($|N| = \max\{1, q-(t-1)R\}$) is arbitrary and so are the $(t-1)$ different elements $a_2, a_3, \ldots, a_t \in F_q \setminus \{0\}$. We now show that this

construction can be further improved for $R \geq 2$, since the first column of $\mathbf{A}$ is then superfluous. In the proof of the following theorem we only show how to modify the proof of [10, Theorem 3].

Theorem 7 *Let $s = \max\{1, q-(t-1)R\}$. If q is a prime and $R \geq 2$, then $K_q(tn, R) \leq sq^{(t-1)n-1}K_q(n, R)$.*

Proof: Take any (x, y), where $x \in F_q$, $y \in F_q^n$. Now, since C is a $(q, n, M)R$ code, there is a codeword $c \in C$, such that $d(y, c) = k \leq R$. In the case $k = R$, the first column in A is not used in the proof of [10, Theorem 3]; we can thus proceed with the case $k < R$. If $k < R$, then for any $b \in N$,

$$(x, y)^T = (b, c)^T + (x - b)A_1 + \sum_{j=1}^{k} \alpha_j A_{1+i_j}, \tag{1}$$

where A_i is the ith column of $\mathbf{A}$, and i_j is the jth nonzero coordinate of $y - c$. If $x \neq b$, the first column of $\mathbf{A}$ is used. We now choose $a_2 = 1$ to get $A_1 = (q-1)A_{1+i_j} + A_{1+i_j+n}$ for any i_j. If $k \geq 1$, we can rewrite (1) as

$$(x, y)^T = (b, c)^T + ((q-1)(x-b)+\alpha_1)A_{1+i_1} + (x-b)A_{1+i_1+n} + \sum_{j=2}^{k} \alpha_j A_{1+i_j}, \tag{2}$$

which uses $k + 1 \leq R$ columns of $\mathbf{A}$. If $k = 0$, A_1 can be expressed as a weighted sum of two other columns in the same way, so for the construction to work we must have $R \geq 2$. Together with the details in [10, Theorem 3], this completes the proof. □

Now [10, Corollary 5] can also be improved: If q is a prime and $R \geq \max\{2, q-1\}$, then $K_q(2n, R) \leq q^{n-1}K_q(n, R)$. Thus, by starting from the ternary Golay code we get that $K_3(22, 2) \leq 3^{10}K_3(11, 2) = 3^{16}$, thereby "saving one coordinate" compared to the result in [10] ($K_3(23, 2) \leq 3^{17}$, which immediately follows from our result).

It is not difficult to see that if the original code is a linear code and $s = 1$ ($N = \{0\}$), then the code obtained by this construction is also linear. Linear ternary covering codes have recently been studied in [6]. Let $l(r, R; q)$ denote the minimum length of a q-ary linear code of co-dimension r ($= n - k$) and covering radius R. The new construction gives that if q is a prime and $R \geq \max\{2, q-1\}$, then $l(r+1, R; q) \leq 2l(r, R; q)$, which leads to several improvements in [6, Table I]: $l(6, 2; 3) \leq 22$, $l(12, 2; 3) \leq 646$, $l(14, 2; 3) \leq 1942$, $l(16, 2; 3) \leq 5830$, $l(18, 2; 3) \leq 17468$, $l(20, 2; 3) \leq 52406$, $l(22, 2; 3) \leq 157220$, and $l(24, 2; 3) \leq 471662$.

In [10] the case when q is a prime power is also considered. Slight improvements on [10, Theorems 7 and 8] can be obtained using arguments similar to those in the proof of Theorem 7.

5. Tables of Upper Bounds

Upper bounds for 3-ary, 4-ary, and 5-ary covering codes are given in Tables I, II, and III, respectively. Unmarked entries are collected from [16]. Marked entries are those bounds which have been improved since [16] appeared—there are 23 such bounds—and old bounds which have been given a nice new construction (possibly in this paper). Constructions of ternary codes can also be found in [21]. Lower bounds are not given, but known exact values are indicated by a period. These are from [5], except for $K_3(5,2) = 8$, which is from [21].

In [4, Remark 4.2(b)] it is claimed that $K_5(7,2) \leq 500$, which is slightly better than $K_5(7,2) \leq 525$ proved here. Unfortunately, the proof of [4, Theorem 4.1]—which claims that $K_q(n+1, R+1) \leq (q-1)q^{k-1}$ if there is a linear $(q, n, q^k)R$ code—is incorrect and cannot be used to prove the bound. For example, by applying this theorem to the ternary Hamming code of length 4, we get that $K_3(5,2) \leq 6$, but from Table I we can see that $K_3(5,2) = 8$. The proof contains elementary errors. None of the correct upper bounds given in [4] improve on the upper bounds in Tables I–III.

Key to Tables I, II, and III.

a Published in the Finnish magazine *Veikkaaja* 47/1960; constructed by Aarne Lahtinen.
ci Corollary i.
d $K_q(n+1, R) \leq qK_q(n, R)$.
m Matrix method.
ri Reference [i].
ti Theorem i.

TABLE I. Upper bounds on $K_3(n,R), 1 \leq n \leq 14, 1 \leq R \leq 9$

$n\backslash R$	1	2	3	4	5	6	7	8	9
1	1.								
2	3.	1.							
3	5.	3.	1.						
4	9.	3.	3.	1.					
5	27.	8.	3.	3.	1.				
6	73	17	6.	3.	3.	1.			
7	186	34	12	3.	3.	3.	1.		
8	486	81	27	9	3.	3.	3.	1.	
9	1341^{r20}	219	54	18	6	3.	3.	3.	1.
10	3645	558	108	36	12	3.	3.	3.	3.
11	9477^{r19}	729.	243	81	27	9	3.	3.	3.
12	27702^{r19}	2187	729	204	54^{a}	18	6	3.	3.
13	59049.	6561	1215^{r17}	408^{r17}	108^{t5}	45^{t5}	12	3.	3.
14	177147	19683	2187	729^{r17}	243^{m}	81^{m}	27	9	3.

TABLE II. Upper bounds on $K_4(n,R), 1 \leq n \leq 10, 1 \leq R \leq 7$

$n\backslash R$	1	2	3	4	5	6	7
1	1.						
2	4.	1.					
3	8.	4.	1.				
4	24.	7.	4.	1.			
5	64.	16^{c1}	4.	4.	1.		
6	256	52^{m}	16	4.	4.	1.	
7	1024	128^{m}	32^{c3}	12	4.	4.	1.
8	3456^{m}	384^{m}	96^{c3}	28^{c3}	8	4.	4.
9	12288^{m}	1024^{r3}	256	64^{c3}	16^{c3}	4.	4.
10	49152^{d}	4096	1024	208^{c3}	64	16	4.

TABLE III. Upper bounds on $K_5(n,R), 1 \leq n \leq 9, 1 \leq R \leq 7$

$n\backslash R$	1	2	3	4	5	6	7
1	1.						
2	5.	1.					
3	13.	5.	1.				
4	51	11^{r18}	5.	1.			
5	184	35	9^{r18}	5.	1.		
6	625.	125^{c1}	25^{c1}	5.	5.	1.	
7	3125	525^{m}	125	25	5.	5.	1.
8	15625	1875^{m}	325^{t4}	65^{c3}	20	5.	5.
9	78125	7500^{m}	1275^{t4}	255^{c3}	55^{c3}	15	5.

Acknowledgment

The author is grateful to Rene Struik whose valuable suggestions improved the paper. The author thanks George Kennedy for reporting the existence of a $(3, 14, 3^5)5$ linear code, and Heikki Hämäläinen for reporting the existence of a $(3, 12, 54)5$ code, constructed by Aarne Lahtinen in 1960.

Appendix

Codes obtained by the matrix method are listed here. For each code, the columns of the M matrix are first listed, followed by the words in S. These two sets are separated by a semi-colon. For $q = 4$, we denote $F_4 = \{0, 1, 2 = \alpha, 3 = \alpha^2\}$, where α is a primitive element; for $q = 2, 3, 5$, we let $F_q = \{0, \ldots, q-1\}$ and operate on this set modulo q.

$K_2(14, 1) \leq 1408$: 110000000, 101000000, 011000000, 100111000, 011000111; 000001111, 000010011, 000010101, 000011000, 000101001, 000111110, 001000001, 001001000, 001010000, 001111010, 001111101, 010000111, 010011110, 010100010, 010101100, 010110100, 010111011, 011000110, 011001011, 011001101, 011010001, 011100000, 011110111, 100000010, 100000100, 100001001, 100100110, 100110001, 101001110, 101010110, 101011111, 101100011, 101100100, 110000000, 110011001, 110100101, 110101010, 110110010, 110111100, 111010111, 111011010, 111011100, 111101111, 111111000.

$K_3(14, 5) \leq 243$: 111111000, 211100110, 021021210, 121010101, 220201011; 000000000.

$K_3(14, 6) \leq 81$: 1111111000, 2211100110, 1021021210, 1221010101; 0000000000.

$K_4(8, 1) \leq 3456$: 11100, 32100, 23100; 00122, 00131, 01321, 01332, 02001, 02010, 02033, 03200, 03212, 03223, 10122, 10131, 11201, 11210, 11233, 12300, 12312, 12323, 13021, 13032, 20122, 20131, 21000, 21012, 21023, 22221, 22232, 23301, 23310, 23333, 30003, 30011, 30030, 30100, 30103, 30110, 30113, 30122, 30131, 30203, 30211, 30230, 30303, 30311, 30330, 31102, 31113, 31120, 32102, 32113, 32120, 33102, 33113, 33120.

$K_4(9, 1) \leq 12288$: 1100, 1010, 1001, 0111, 1111; 0133, 0221, 1000, 1312, 2102, 2210, 3011, 3023, 3120, 3232, 3303, 3331.

$K_4(6, 2) \leq 52$: 11111; 00031, 00323, 03100, 10210, 12133, 12302, 22020, 23232, 23311, 31003, 31112, 31221, 31330.

$K_4(7, 2) \leq 128$: 11100, 32100; 02202, 02231, 10113, 10120, 21301, 21332, 33010, 33023.

$K_4(8, 2) \leq 384$: 11100, 32111, 21321; 02132, 10232, 21032, 33303, 33311, 33320.

$K_5(7,2) \leq 525$: 11100, 11010; 03324, 04214, 12320, 13213, 14210, 14431, 21100, 21321, 23101, 24041, 30102, 31042, 32432, 33043, 33212, 33321, 40044, 40433, 41430, 42323, 44104.
$K_5(8,2) \leq 1875$: 11100, 32100, 43110; 00144, 01221, 03442, 04003, 11423, 14200, 20041, 22202, 24404, 30243, 31324, 33020, 40440, 41022, 44301.
$K_5(9,2) \leq 7500$: 11000, 21000, 31000, 41110; 01001, 01122, 10003, 10132, 10213, 24142, 24210, 33211, 33424, 42000, 42124, 42344.

References

[1] A. Blokhuis and C. W. H. Lam, More coverings by rook domains, *J. Combin. Theory Ser. A* **36** (1984), 240–244.

[2] R. C. Bose, S. S. Shrikhande, and E. T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture, *Canad. J. Math.* **12** (1960), 189–203.

[3] R. A. Brualdi, V. S. Pless, and R. M. Wilson, Short codes with a given covering radius, *IEEE Trans. Inform. Theory* **35** (1989), 99–109.

[4] W. A. Carnielli, Hyper-rook domain inequalities, *Stud. Appl. Math.* **82** (1990), 59–69.

[5] W. Chen and I. S. Honkala, Lower bounds for q-ary covering codes, *IEEE Trans. Inform. Theory* **36** (1990), 664–671.

[6] A. A. Davydov, Constructions and families of covering codes and saturated sets of points in projective geometry, *IEEE Trans. Inform. Theory* **41** (1995), 2071–2080.

[7] S. W. Golomb and E. C. Posner, Rook domains, Latin squares, affine planes, and error-distributing codes, IEEE Trans. Inform. Theory **10** (1964), 196–208.

[8] H. Hämäläinen and S. Rankinen, Upper bounds for football pool problems and mixed covering codes, *J. Combin. Theory Ser. A* **56** (1991), 84–95.

[9] I. S. Honkala, On (k,t)-subnormal covering codes, *IEEE Trans. Inform. Theory* **37** (1991), 1203–1206.

[10] I. S. Honkala, On lengthening of covering codes, *Discrete Math.* **106/107** (1992), 291–295.

[11] H. J. L. Kamps and J. H. van Lint, A covering problem, *Colloq. Math. Soc. János Bolyai* **4** (1970), 679–685.

[12] G. Kennedy, personal communication.

[13] J. H. van Lint Jr., "Covering Radius Problems," M.Sc. Thesis, Eindhoven University of Technology, The Netherlands, 1988.

[14] J. H. van Lint Jr. and G. J. M. van Wee, Generalized bounds on binary/ternary mixed packing- and covering codes, *J. Combin. Theory Ser. A* **57** (1991), 130–143.

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

[16] P. R. J. Östergård, Upper bounds for q-ary covering codes, *IEEE Trans. Inform. Theory* **37** (1991), 660–664; and 37 (1991), 1738.

[17] P. R. J. Östergård, Further results on (k,t)-subnormal covering codes, *IEEE Trans. Inform. Theory* **38** (1992), 206–210.

[18] P. R. J. Östergård, Construction methods for mixed covering codes, in: M. Gyllenberg and L. E. Persson (eds.), "Analysis, Algebra, and Computers in Mathematical Research; Proceedings of the 21st Nordic Congress of Mathematicians," Marcel Dekker, New York, 1994, pp. 387-408.

[19] P. R. J. Östergård, New upper bounds for the football pool problem for 11 and 12 matches, *J. Combin. Theory Ser. A* **67** (1994), 161-168.

[20] P. R. J. Östergård, Constructing covering codes by tabu search, *J. Combin. Des.*, to appear.

[21] P. R. J. Östergård and H. O. Hämäläinen, New upper bounds for binary/ternary mixed covering codes, *Des. Codes Cryptogr.*, to appear.

[22] R. C. Singleton, Maximum distance q-ary codes, *IEEE Trans. Inform. Theory* **10** (1964), 116–118.

[23] G. J. M. van Wee, Bounds on packings and coverings by spheres in q-ary and mixed Hamming spaces, *J. Combin. Theory Ser. A* **57** (1991), 117–129.