COVERINGS BY R-DIMENSIONAL ROOK DOMAINS

E. L. Monte Carmelo *

Dedicated to the Prof. Jayme L. Szwarcfiter, on the occasion of his 60^{th} birthday.

Abstract

Based on the matrix method, constructions of q-ary code of length n and covering radius R are established. One generalizes a theorem due to Blokhuis and Lam, and also improves a result by van Lint Jr; while another extends a construction by Carnielli.

1 Introduction

Given the set V_q^n of all words with length n and components from the ring $\mathbb{Z}_q$ (or the field $\mathbb{F}_q$, when q is a prime power), the *R-dimensional rook domain* of x is defined as the set of all vectors y in V_q^n which differ from x in at most R coordinates, i.e., $\{y \in V_q^n : d(x,y) \leq R\}$, where d denotes the Hamming distance. If V_q^n can be represented as the union of R-dimensional rook domain of the vectors in $C \subset V_q^n$, then we say that C *R-covers* V_q^n (or C is an R*-covering set of* V_q^n) and we call the elements in C by *rook*.

In this note we focus on the numbers

$$K_q(n, R) = \min\{\ |C| :\ C\ R\text{-covers } V_q^n\ \}$$

which was initially posed for $R = 1$ by Taussky and Todd [9] in terms of abelian groups, and generalized for arbitrary R by Carnielli [2]. The determination of these numbers has resisted a series of mathematical and computational attacks for more than 50 years. Indeed, besides a list of particular classes, exact values are known for small entries (see [4]). However, there is substantial progress

Keywords: bounds on codes, lengthening of covering codes, matrix method, dominating set. **MSC 2000:** 05B40 and 94B65.

*Research partially supported by CAPES-Brazil

on bounds for several classes and instances, and bounds has been periodically updated in tables when q and n are small (see [4]).

Many of such upper bounds are derived by inductive relations, which produce new R-covering codes from old s-covering codes, where $0 < s < R$. In this note, we are concerned with the following theoretical question: how to obtain new R-covering codes using only R-covering codes?

The first inductive relation (section 3) generalizes a theorem due to Blokhuis and Lam [1], and improves also a theorem by van Lint Jr. [7], while another extends one by Carnielli [3]. Both constructions are based on the matrix method (see next section), which is reduced to the dominating set.

2 Matrix method and dominating set

For the sake of our purposes, we recall the following well-known results on $K_q(n,R)$ (see [4], for instance).

Lemma 1 *For every q and n,*

(a) $K_q(n,0) = q^n$ *and* $K_q(n,n) = 1$;

(b) $K_q(2,1) = q$ *and* $K_q(3,1) = \lceil q^2/2 \rceil$;

(c) for a prime power q and n such that $1+(q-1)n = q^t$, we have $K_q(n,1) = q^{n-t}$ (perfect codes).

The direct sum construction yields the following relations (see [2] or [4]).

Lemma 2

(a) $K_q(m+n, R_1+R_2) \leq K_q(m,R_1)K_q(n,R_2)$,

(b) $K_q(m+n,R) \leq q^m K_q(n,R)$.

We now describe the main tool, so-called *matrix method,* whose origin is due to Kamps and van Lint [6]. This approach was later refined and systematized for the case $R = 1$ by Blokhuis and Lam [1], and generalized for arbitrary R in [3, 7].

Let $A = (I_k; M) = (a_1, a_2, ..., a_m)$ be an $k \times m$ matrix, where I_k denotes the $k \times k$ identity matrix and M is a $k \times (m-k)$ matrix with entries from $\mathbb{Z}_q$. A subset S of V_q^k is called an *R-covering of V_q^k using A* iff any x in V_q^k can be written as a sum of a vector $s \in S$ and a $\mathbb{Z}_q$-linear combination of at most R columns of A, i.e.,

$$x = s + \alpha_1 a_{l_1}^T + \alpha_2 a_{l_2}^T + \cdots + \alpha_R a_{l_R}^T,$$

where $s \in S$, and z^T denotes the transpose of the column z in A. Since the canonical vectors are also columns in A, note that S R-covers V_q^k coincides with the case where $A = I_k$.

Theorem 3 *[3, 7] If S is an R-covering of V_q^k using a $k \times m$ matrix $A = (I_k; M)$, then*

$$K_q(m, R) \leq |S| \, q^{m-k}.$$

Example: The set $S = \{(0,0), (1,1)\}$ does not 1-cover V_3^2, because $d(x, (2,2))=$ 2 for any x in S. However, it is an 1-covering of V_3^2 using the matrix

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

Theorem 3 yields $K_3(3,1) \leq 6$ (the exact value follows from Lemma1.b).

The problem of deciding whether S is an R-covering of V_q^k using a suitable matrix can be restated in terms of graph theory, as described below.

Let $G = (V, E)$ be an undirected graph with vertex set V and edge set E. The subset $S \subset V$ is said to be a *dominating set* of G iff, for every vertex v in V, either $v \in S$, or there is a vertex $s \in S$ such that s is adjacent to v.

Proposition 4 *Covering set using matriz is equivalent to the dominating set for a class of graphs.*

Proof: Fixed k, q, R, and a matrix $A = (I_{k;}\ M)$, let us construct the graph $G = (V, E)$ as follows: take $V = V_q^k$, and, for two points $x \neq y$ in V, define x is adjacent to y if and only if $x - y$ is a $\mathbb{Z}_q$-linear combination of at most R columns of A. Since $-1 \in \mathbb{Z}_q$, G is an undirected graph. Note that to say that S is an R-covering of V_q^k using A is equivalent to say that S is a dominating set of G.

□

As an immediate consequence, the number $K_q(k, R)$ can be evaluated by solving the minimum dominated set problem on the graph $G = G(k, q, R, I_k)$.

3 The constructions

Let us introduce the following notation: I_v denotes the identity matrix of order v.

Theorem 5 *For any prime power q and $R \geq 1$,*

$$K_q(q(n-R+1)+R, R) \leq q^{(q-1)(n-R+1)} K_q(n, R).$$

Proof: Let C be a minimal R-covering set on V_q^n containing the zero vector (this is always possible by adding a suitable vector to the covering set). Take $S = C \times \{0\} \subset V_q^{n+1}$ and consider the following $(n+1) \times (q-1)(n-R+1)+(n+1)$ matrix:

$$A = \begin{bmatrix} & 1I_{n-R+1} & 2I_{n-R+1} & \dots & (q-1)I_{n-R+1} \\ I_{n+1} & \overline{0} & \overline{0} & \dots & \overline{0} \\ & \overline{1} & \overline{1} & \dots & \overline{1} \end{bmatrix}$$

where I_{n+1} denotes the identity matrix of order $n+1$, $\overline{0}$ represents the $(R-1) \times (n-R+1)$ zero matrix, and $\overline{1}$ denotes the $1 \times (n-R+1)$ matrix whose all entries are 1. Here $\mathbb{F}_q = \{0, 1, \dots, q-1\}$.

We apply Theorem 3 with $k = n+1$ and $m = q(n-R+1)+R$. We claim that S R-covers V_q^{n+1} using A. Indeed, let each vector w in V_q^{n+1} be written as $w = (x; t)$, where $x \in V_q^n$ and $t \in \mathbb{F}_q$. By construction, there is $(s; 0)$ in S which disagrees with $(x; 0)$ in at most R coordinates, say that

$$(x; 0) = (s; 0) + \alpha_1 e_{l_1} + \alpha_2 e_{l_2} + \cdots + \alpha_d e_{l_d} \quad (1)$$

where $d \leq R$, $\alpha_i \in \mathbb{F}_q$, and e_{l_i} are columns in I_{n+1}. If $t = 0$, then w is covered by S, according to (1). For the case $t \neq 0$ and $d < R$, we can represent w as

$$w = (s; 0) + te_{n+1} + \alpha_1 e_{l_1} + \alpha_2 e_{l_2} + \cdots + \alpha_d e_{l_d}.$$

We now examine the last case $t \neq 0$ and $d = R$. Since the R canonical vectors in (1) are distinct to e_{n+1}, by pigeonhole principle, there is an index, say l_1, such that $1 \leq l_1 \leq n-R+1$. Hence

$$w = (s; 0) + t\left(e_{n+1} + t^{-1}\alpha_1 e_{l_1}\right) + \alpha_2 e_{l_2} + \cdots + \alpha_R e_{l_R}$$

is a required representation, because the vector $(e_{n+1} + t^{-1}\alpha_1 e_{l_1})^T$ is a column of A. The result follows from Theorem 3.

□

In particular, when q is a prime and $R = 1$, Theorem 5 reduces to [1, Theorem 4.1].

Corollary 6 *[7] For a prime power q and $R \geq 1$,*

$$K_q(qn + 1, R) \leq q^{n(q-1)} K_q(n, R).$$

Proof: Apply Theorem 5 and Lemma 2.b with $m = (q - 1)(R - 1)$.

□

Therefore, Theorem 5 improves m coordinates on the above relation. The construction given by van Lint Jr. (see also [4, Theorem 3.5.3]) can be improved under certain conditions, according to [5].

Corollary 7 *For all $R \geq 1$,*

$$K_2(2n - R + 2, R) \leq 2^{n-R+1} K_2(n, R).$$

The case $R = 1$ coincides with the very useful relation $K_2(2n + 1, 1) \leq 2^n K_2(n, 1)$ (see [4, Theorem 3.4.3]).

Some ideas arising from the proof of Theorem 5 can be applied to extend [3, Theorem 3.9], as follows.

Theorem 8 *Given a prime power q, put $n = R + K_q(R, R) + K_q(R + 1, R) + K_q(R + 2, R) + \cdots + K_q(r - 1, R)$. We have*

$$K_q(n, R) \leq [1 + (q - 1)(r - R)]\, q^{n-r}.$$

Proof: Take $S = \{\alpha e_j : \alpha \in I\!F_q \text{ and } 2 \leq j \leq r - R + 1\} \subset V_q^r$ and

$$A = \left[\begin{array}{ccccc}
0 & 0 & \cdots & 1 & 0_R \\
0 & 0 & \cdots & K_q(r-1, R) & 0_R \\
0 & \vdots & & * & \\
\vdots & 0 & \cdots & & \vdots \\
0 & 1 & \cdots & & \\
1 & K_q(R+1, R) & \cdots & & 0_R \\
K_q(R, R) & * & \cdots & \vdots & -- \\
* & \vdots & & & \\
\vdots & \vdots & & & I_R \\
* & * & \cdots & * &
\end{array}\right]$$

Here, for any i such that $R \leq i \leq r-1$, $C_i = [0 \cdots 01\ K_q(i,R) * \cdots *]^T$ represents the $K_q(i,R) \times r$ submatrix composed by all columns $(0, \cdots, 0, 1, v)^T$, where v denotes a rook from a minimal R-covering on V_q^i containing the zero vector. The submatrix $[O_R \cdots O_R; I_R]^T$ is composed by the transpose of the vectors $e_{r-R+1}, e_{r-R+2}, \cdots, e_r$ in V_q^r.

Note that e_i appears in C_{r-i} for $1 \leq i \leq r-R$, and so all the canonical vectors in V_q^r appear as columns in A, i.e, I_r is a submatrix of $A_{r\times n}$.

Now, we apply Theorem 3 using $k=r$ and $m=n$. It is sufficient to show that S is an $R-$covering of V_q^r using A. Indeed, the zero vector is covered by S. Otherwise, let $w = (0, 0, \cdots, 0, w_1, w_2, \cdots, w_i)$ be an arbitrary vector in $V_q^r \backslash \{0\}$, where the first $r-i$ coordinates are zero and $w_1 \neq 0$, for one i, $1 \leq i \leq r$.

We analyse some cases. Case 1: if $i \leq R$, then $w = 0 + w_1 e_{r-i+1} + w_2 e_{r-i+2} + \cdots + w_i e_r$ has the desired form. Case 2: if $i \geq R+1$. Let β be the inverse of w_1. By construction of A, there is a column v^T in C_{i-1}^T such that

$$\beta w = v + \alpha_1 e_{l_1} + \alpha_2 e_{l_2} + \cdots + \alpha_s e_{l_s} \tag{2}$$

for some $s \leq R$, where e_{l_i} denotes suitable canonical vector in I_r. Case 2.1: if $s < R$, thus w is a linear combination of $s+1 \leq R$ columns of A. Case 2.2: $s = R$, without loss of generality, suppose that e_{l_1} has the last $R-1$ coordinates equal to 0, because there are R unitary vectors in (2). Then

$$w = \beta^{-1}\alpha_1 e_{l_1} + \beta^{-1} v + \beta^{-1}\alpha_2 e_{l_2} + \cdots + \beta^{-1}\alpha_R e_{l_R}$$

where $\beta^{-1}\alpha_1 e_{l_1}$ belongs to S, because $2 \leq l_1 \leq r-R+1$.

Each $\alpha \in \mathbb{F}_q$, $\alpha \neq 0$, produces $r-R$ vectors in S, while $\alpha = 0$ yields only the null vector. Then $|S| = 1 + (q-1)(r-R)$, and the proof is complete.

□

Example: We recall the following values: $K_2(1,1) = 1$, $K_2(2,1) = 2$, $K_2(3,1) = 2$, $K_2(4,1) = 4$, $K_2(5,1) = 7$, $K_2(6,1) = 12$, and $K_2(7,1) = 16$ (see table in [4]). Applying Theorem 8 for $q=2$, $R=1$ and $r=8$, we obtain $K_2(45,1) \leq 2^{40}$, which is equivalent to 16/15 of the current bound $K_2(45,1) \leq 15.2^{36}$. However, as in many instances, this estimate was obtained using a non-systematical combinations of relations and existence of special codes. Indeed, $K_2(45,1) \leq 2^2 K_2(43,1)$, by Lemma 2.b, while $K_2(43,1) \leq 2^{21} K_2(21,1)$, by Corollary 7, which also implies $K_2(21,1) \leq 2^{10} K_2(10,1)$. Finally, $K_2(10,1) \leq 15.2^3$ is derived from a particular construction based on a strongly seminormal code, according to [8].

Acknowlegments. The author would like to thank the anonymous referees, for several remarks which lead to the improvement of the present version.

References

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

[2] Carnielli, W. A., *On covering and coloring problems for rook domains*, Discrete Math. 57 (1985), 9-16.

[3] Carnielli, W. A., *Hyper-rook domain inequalities*, Stud. Appl. Math. 82 (1990), 50-69.

[4] Cohen, G., Honkala, I., Litsyn, S., Lobstein, A., *Covering codes.* (North-Holland, Amsterdam, 1997).

[5] Honkala, I., *On lengthening of covering codes*, Discrete Math. 106/107 (1992), 11-18.

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

[7] van Lint Jr., J. H., *Covering radius problems*, M.Sc. thesis, Eindhoven University of Technology, The Netherlands (1988).

[8] Östergård, P. R. J.; Kaikkonen, M. K., *New upper bounds for binary covering codes*, Discrete Math. , 178 (1998), 165-179.

[9] Taussky, O.; Todd, J., *Covering theorems for groups*, Ann. Soc. Polonaise Math., 21 (1948), 303-305.

E. L. Monte Carmelo
Departamento de Matemática
Universidade Estadual de Maringá
Av. Colombo, 5790
87020-900, Maringá, PR, Brazil
E-mail: elmcarmelo@uem.br