Covering codes and invariant sets

E.L. Monte Carmelo

***Abstract*— Let $c_q(n,R)$ denote the minimum cardinality of a subset H in $\mathbb{F}_q^n$ such that every word in this space differs in at most R coordinates from a multiple of a vector in H, where q is a prime power. In order to explore the symmetries of such coverings, a few algebraic properties of invariant sets under certain translation are investigated. As an application, a new class of upper bounds on $c_q(n,R)$ is reported, extending a previous result by Mendes et al. Moreover, the new upper bound on the classical covering $K_q(qr, qr-r-1) \leq 2q-1$ for a prime power $q \geq r+3$ is derived too, improving a bound by Östergård.**

***Index Terms*— invariant set, finite field, translation, covering code, bounds on codes.**

I. Introduction

Let $K_q(n,R)$ denote the minimal cardinality of an R-covering code over the n-th power of an alphabet with q symbols (see precise definition in Section IV). The determination of these numbers seem to be a great challenge of combinatorial coding theory. Indeed, covering codes have been extensively investigated during the last 60 years, since the seminal paper by Taussky and Todd [20].

An interesting application corresponds to the case $q=3$ and $R=1$, because the number $K_3(n,1)$ gives us the best way of guaranteeing $n-1$ correct forecasts in a football pool with n matches.

Many concepts and variants (for instance, covering using the matrix method [2], normal and subnormal codes [5], [8]) have been studied in order to shed light on the computation of $K_q(n,R)$. See an overview on covering codes and applications in [3].

A recent variant is described below. Let $\mathbb{F}_q^n$ denotes the n-dimensional vector space over the finite field $\mathbb{F}_q$, where q denotes a prime power. A subset H of $\mathbb{F}_q^n$ is an R-short covering of $\mathbb{F}_q^n$ iff any x in $\mathbb{F}_q^n$ can be written as a sum of a scalar multiple of $h \in H$ and a linear combination of at most R canonical vectors. The number $c_q(n,R)$ is defined as the minimum cardinality of an R-short covering of $\mathbb{F}_q^n$.

Some of the motivations for studying short covering codes are listed below:

- Short coverings provide us a way to store coverings using less memory than the classical ones. This may be useful for nonlinear codes in spaces over large q.
- On the basis of theoretical viewpoint, the behavior of short coverings seems to be interesting too. Short coverings have been connected with some branches of mathematics and computer science: group theory (actions of group), combinatorial number theory (sum-free sets), extremal problems, graph theory (dominating set), and local search (tabu search); according to [12], [14], [15], [16].
- Results on short covering codes might be a able to bring us record-breaking on the classical codes. Indeed, several results on $c_q(n,R)$ have been obtained in [16] on the basis of information about $K_q(n,R)$. In another direction, the work [12] explores a new upper bound on $K_q(n,R)$ from short covering code, which yields $K_5(10,7)=9$ from the value $c_5(10,7)=2$.

This work concerns on the numbers $c_q(n,R)$ and their relationships with $c_q(n,R)$, more precisely, the goals of this work are as follows:

- A new method based on invariant sets under suitable permutation is discussed. For this purpose, the concept γ-path is introduced, which plays a central role in our results. As a consequence, a new exact class of short coverings is constructed from this method, extending the construction for $c_5(10,7)=2$.
- Moreover, this approach may be applied to the classical covering too, which also yields the new upper bound class $K_q(qr, qr-r-1) \leq 2q-1$ for a prime power $q \geq r+3$, improving the previous upper bound by Östergård [18].

This note is organized as follows. In Section II, we describe the numbers $c_q(n,R)$ and review some of the previous results. The main result is reported in Section III, and it is applied to get a new class of classical covering codes in Section IV. The main tool of our results is outlined in Section V, where results on invariant sets under a translation are investigated. A comparative analysis between classical and short covering concludes this work.

Proof of all results and further material can be found in [13].

II. Short covering codes: review of some results

A. Problem Formulation

Short coverings are described more formally in this section. Given a vector h in the space $\mathbb{F}_q^n$, and $0 \leq R \leq n$, let

$$E(h,R) = \bigcup_{\alpha \in \mathbb{F}_q} \left\{ \alpha h + \sum_{i=1}^{R} \alpha_i e_{l_i} : \ 1 \leq l_i \leq n, \ \alpha_i \in \mathbb{F}_q \right\},$$

where e_{l_i} denotes the l_i-th canonical vector in $\mathbb{F}_q^n$, with $1 \leq l_i \leq n$, where $1 \leq i \leq n$. A subset H of $\mathbb{F}_q^n$ is an *R-short*

This work was partially supported by CNPq/MCT.

E. L. Monte Carmelo is with the Departamento de Matemática, Universidade Estadual de Maringá, Paraná, Brazil. elmcarmelo@uem.br

covering (or *R-short covering code*) of $\mathbb{F}_q^n$ when

$$\bigcup_{h\in H} E(h,R) = \mathbb{F}_q^n.$$

In other words, H is an R-short covering of $\mathbb{F}_q^n$ iff any x in $\mathbb{F}_q^n$ can be written as a sum of a scalar multiple of $h \in H$ and a linear combination of at most R canonical vectors. The induced extremal problem is defined as follows

$$c_q(n,R) = \min\{|H| : H \text{ is an } R\text{-short covering of } \mathbb{F}_q^n\}.$$

B. A few known results

Let us repot a few results on the numbers $c_q(n,R)$ obtained in [16]. We begin stating general lower and upper bounds on short covering codes.

Proposition 1: For a prime power q, and every n and R such that $0 \leq R < n$,

$$\left\lceil \frac{q^n - v}{(q-1)v} \right\rceil \leq c_q(n,R) \leq \frac{q^{n-R}-1}{q-1},$$

where

$$v = 1 + \sum_{i=1}^{R} \binom{n}{i}(q-1)^i.$$

The lower bound is closely related to the well-known sphere-covering bound for $K_q(n,R)$. Information on covering codes can give us a preliminary idea about the behavior of short covering code. For instance, the above bound is attained at least in the case where coverings are derived from Hamming codes, according to the next result.

Theorem 2: For every prime power q, and every positive integers t and n such that $n = (q^t-1)/(q-1)$,

$$c_q(n,1) = \frac{q^{n-t}-1}{q-1}.$$

However, neither lower bound nor upper bound is sharp in Proposition 1 for the next instance.

Example 3: We have $c_3(3,1) = 3$.

It is expected that lower and upper bounds in Proposition 1 are far from the exact value in many cases. It is worth mentioning that the corresponding trivial bounds on $K_q(n,R)$ are not good for most instances too. In this situation, the contributions have been focused on particular classes or even for an instance of (q,n,R), like in [4] for example.

Theorem 4: We have $n \geq (t-1)q+1$ if and only if

$$c_q(n,n-t) = 1.$$

III. The main statement

Suitable constructions of short covering codes enable us to state new upper bounds, as established in the main result of this work.

Theorem 5: For a positive integer r and a prime power $q \geq r+3$,

$$c_q(qr, qr-r-1) = 2.$$

Proof: Sketch: The lower bound comes from Theorem 4. For the upper bound, let $n = qr$ and $R = qr-r-1$. Choose the following vectors in $\mathbb{F}_q^n$:

$$\begin{aligned} k &= (1,1,\ldots,1,1,\ldots,1) \\ h &= (1,1,\ldots,\xi,\xi,\ldots,\xi), \end{aligned}$$

where ξ denotes a generator of $\mathbb{F}_q^*$ and it appears in the last $r+1$ coordinates of h. We claim that $H = \{k,h\}$ is an R-short covering of $\mathbb{F}_q^n$. Roughly, the proof of the above claim is based on the characterization of invariant sets under certain translation given in Section V. The details of the proof can be found in [13]. ■

Remark 6: We note that:

- Theorem 5 generalizes the previous result $c_q(q,q-2) = 2$, $q \geq 4$, by Mendes et al. [12].
- The hypothesis $q \geq r+3$ is essential, because the result can not be extended to arbitrary q. Indeed, note that $c_3(3,1) = 3$, as mentioned in Example 3.
- In contrast with the above result, the computation of $K_q(q,q-2)$ still remains an open problem for arbitrary q. However, their exact values were determined for $q \leq 10$, according to Hass et al [6].

IV. An application: from short covering to classical covering code

Given two vectors $x = (x_1,x_2,\ldots,x_n)$ and $y = (y_1,y_2,\ldots,y_n)$ in $\mathbb{F}_q^n$, the *Hamming distance* between the words x and y is

$$d(x,y) = |\{i : x_i \neq y_i\}|.$$

In the metric space $\mathbb{F}_q^n$ with the Hamming distance, the *sphere* of center x and *radius* R is denoted by

$$B(x,R) = \{y \in \mathbb{F}_q^n : d(x,y) \leq R\},$$

A subset C is an *R-covering* (or *R-covering code*) of $\mathbb{F}_q^n$ when

$$\bigcup_{c\in C} B(c,R) = V_q^n.$$

The number $K_q(n,R)$ denotes the minimum cardinality of an R-covering of $\mathbb{F}_q^n$.

A closer look reveals that the recent upper bounds on these numbers have been obtained by computer search, according to the updated tables on $K_q(n,R)$ by Kéri [9]. Sometimes structural property is imposed on the code (codes with certain automorphism) in order to reduce the search space, see [4], [19]. Even in this case, constructions are based on computer local search methods like tabu search, simulated annealing or other computational approach.

The most studied cases correspond to small parameters: $q \leq 5$, $n \leq 33$ and $R \leq 10$. In spite of the fact that the case $q \geq 6$ is also interesting (see [11]), the literature for large q is significantly less.

In the next result, we obtain a class of upper bound on $K_q(n, R)$ by a constructive method, without computer search.

Theorem 7: For a positive integer r and a prime power $q \geq r + 3$,

$$K_q(qr, qr - r - 1) \leq 2q - 1.$$

The proof of Theorem 7 can be found in [13].

Example 8: A particular construction of Theorem 7 yields that the set H composed by the nine vectors

0000000000	
1111111111	1111111222
2222222222	2222222444
3333333333	3333333111
4444444444	4444444333

is a 7-covering of $\mathbb{F}_5^{10}$.

Remark 9: A few consequences are listed below.

- Theorem 7 improves the previous bound

  $$K_q(qr, qr - r - 1) \leq 2q,$$

  due to Östergård [18].
- The sharp upper bound $K_5(10, 7) = 9$ in [12] is an particular case of Theorem 7 (see Example 8). The lower bound $K_5(10, 7) \geq 9$ was obtained by Haas et al. [6].
- Theorem 7 yields alternative proof for both upper bounds

  $$K_4(4, 2) = 7 \quad \text{and} \quad K_5(5, 3) = 9$$

  (see tables in [3] or [9]). The previous constructions by Östergård [17] were based on matrix s-surjective in the context of mixed covering code.

Theorem 10 ([1]): The inequality holds

$$K_q(n_1+n_2, R_1+R_2+1) \geq \min\{K_q(n_1, R_1),\ K_q(n_2, R_2)\}.$$

Near-optimal values may be determined too, for instance,

Corollary 11: We have

$$11 \leq K_7(14, 11) \leq 13$$

Proof: The upper bound follows from Theorem 7. On the other hand, the lower bond is derived by combining Theorem 10 and the value $K_7(7, 5) = 11$, by Kéri and Östergård [11]. ∎

V. Main tool: Invariant sets

Since invariant set under permutation is the main tool in this work, let us review briefly a few concepts on group theory. We recommend the books [7] for details on this theory.

As usual, a family of all the permutations of $\mathbb{F}_q$ is called the *symmetric group* on $\mathbb{F}_q$ and it is denoted by $S_{\mathbb{F}_q}$. If Δ is a nonempty subset of $\mathbb{F}_q$ and $\gamma \in S_{\mathbb{F}_q}$, write

$$\gamma(\Delta) = \{\gamma(v) \ : \ v \in \Delta\}.$$

We say that Δ is *setwise invariant* (or simply *invariant*) under γ iff $\gamma(\Delta) = \Delta$. In the special case where $\Delta = \{a\}$, we also say that γ *fixes* a, that is, $\gamma(a) = a$.

Given r, $2 \leq r \leq q$, a permutation γ in $S_{\mathbb{F}_q}$ is called an r*-cycle* if there are r distinct points $a_1, a_2, \ldots, a_r$ in $\mathbb{F}_q$ such that: $\gamma(\ a_i) = a_{i+1}$, for $1 \leq i \leq r - 1$, $\gamma(\ a_r) = a_1$, and γ leaves all others points fixed. By convention, any 1*-cycle* (a) denotes the identity in $\mathbb{F}_q$.

Example 12: The permutation

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 4 & 2 & 5 & 1 & 0 & 3 & 6 \end{pmatrix}$$

on the finite field $\mathbb{F}_7 = \mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$ may be written as product of disjoint cycles, namely,

$$\gamma = (1, 4).(2).(3, 5, 0, 6) = (1, 4).(3, 5, 0, 6),$$

if we use the convention that elements which are not explicitly mentioned are fixed points.

A well-known result is stated below, which proof may be found in [7].

Lemma 13: Every permutation is a product of disjoint cycles. This decomposition is unique up the order of the cycles.

A. Paths

New concepts are introduced.

Definition 14: Let γ be a permutation in $S_{\mathbb{F}_q}$. A γ*-path* is simply a finite sequence $< a_1, a_2, \ldots, a_m >$ of elements in $\mathbb{F}_q$ which are generated by the recursive relation $a_{i+1} = \gamma(a_i)$, where $1 \leq i \leq m - 1$.

Definition 15: Let Δ be a non-empty subset of $\mathbb{F}_q$. We say that the γ-path $< a_1, a_2, \ldots, a_m >$ *crosses* Δ (or is a γ*-path crossing* Δ) if it satisfies the properties:

- the set $\{a_2, \ldots, a_{m-1}\}$ is contained in Δ.
- both extremal points a_1 and a_m do not belong to Δ.

Example 16: Consider the permutation in Example 12. There are two γ-paths crossing $\{1, 3, 6\}$, namely,

$$< 4, 1, 4 > \ \text{and} \ < 0, 3, 6, 5 > .$$

Moreover, the γ-paths

$$< 4, 1, 4 >, \quad < 6, 3, 5 >, \ \text{and} \ < 5, 0, 6 >$$

cross $\{1, 3, 0\}$.

The last concept will help us to check whether certain sets are really short coverings.

The existence of γ-paths crossing Δ is characterized as follows.

Lemma 17: There is a γ-path crossing Δ if and only if Δ is not an invariant set under γ.

B. Invariant sets under a translation

We now focus on the invariant sets under a translation on the multiplicative group $\mathbb{F}_q^*$. This particular class of permutation plays a central role on the constructions of coverings in Theorem 5.

We analyze translation of the following type. Let ξ be a generator of the cyclic group $\mathbb{F}_q^*$. The symbol $\sigma = \sigma_\xi$ denotes the translation on $\mathbb{F}_q^*$ given by: $\sigma(x) = \xi x$ for every x in $\mathbb{F}_q^*$.

It is worth mentioning that there is a bijective correspondence between the set of all the translations on $\mathbb{F}_q^*$ and the set of all the non-singular linear operators on $\mathbb{F}_q$. Indeed, a translation σ on $\mathbb{F}_q^*$ may be extended to a linear operator on $\mathbb{F}_q$ by simply defining $\sigma(0) = 0$. In view of this statement, a non-singular linear operator on $\mathbb{F}_q$ is referred as a translation on $\mathbb{F}_q^*$ in this work.

Lemma 18: Let σ_ξ be the permutation described above. The only invariant sets under σ_ξ are: $\{0\}$, $\mathbb{F}_q^*$, and $\mathbb{F}_q$.

VI. A comparative analysis and conclusions

We begin this section with a comparative analysis between short covering and classical covering code.

The computation of short coverings seems to be more difficult than the classical ones in general case, since new (combinatorial or algebraic) obstacles arise here:

- The cardinality of $B(x, R)$ does not depend on the vector x, in contrast with the cardinality of $E(x, R)$, which depends on the weight of x (see [16]).
- The sets $E(x, R)$ and $E(y, R)$ are highly intersecting, more precisely, this intersection has at least $v = |B(0, R)|$ vectors.
- If C is a covering, thus any translation (with respect to the addition of vector space)

$$z + C = \{z + x : \ x \in C\}$$

  is also a covering. This property is forbidden for an arbitrary translation in the context of short covering.

Besides the reasons mentioned in Introduction, some advantages in studying short covering are listed below:

- While a minimum covering does not have necessarily any algebraic property, a minimum short covering H generates the classical covering

$$\mathbb{F}_q \cdot H = \{\alpha h \ : \ \alpha \in \mathbb{F}_q\},$$

  which is invariant under scalar multiplication.
- There is instance where the computation of short covering code is easier than the classical problem, as noticed in Theorem 5 and remark.

In this work, we present a new constructive method for finding both covering codes and short covering codes. The upper bounds from Theorems 5 and 7 generalize or improve early constructions, as mentioned in the text. It would be interesting applying this method for another instances or classes.

References

[1] M.C. Bhandari and C. Durairajan, A Note on bounds for q-ary covering codes, *IEEE Transactions on Information Theory*, vol. 42(5), 1996, pp 1640–1642.

[2] W.A. Carnielli, Hyper-rook domain inequalities, *Stud. Appl. Math.* vol. 82, 1990, pp 59–69.

[3] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*, North-Holland, Amsterdam; 1997.

[4] G. Gommard and A. Plagne, $K_5(7, 3) \leq 100$, *J. Combin. Theory Ser. A* vol. 104, 2003, pp 365–370.

[5] R.L. Graham and N.J.A. Slaone, On the covering radius of codes, *IEEE Transactions on Information Theory* vol 31, 1985, pp 385–401.

[6] W. Haas, J.C.S Puchta, and J. Quistorff, Lower bounds on covering codes via partition matrices, *J. Combin. Theory Ser A*, vol. 116, 2009, pp 478–484.

[7] I.N. Herstein, *Topics in Algebra*, J. Wiley & Sons, Singapore; 1993.

[8] I.S. Honkala, Lower bounds for binary covering codes, *IEEE Transactions on Information Theory* vol. 34, 1988, pp 326–329.

[9] G. Kéri, *tables for bound on covering codes* , homepage: http://www.sztaki.hu/~keri/, acessed March , 2010.

[10] G. Kéri and P.R.J. Östergård, On the covering radius of small codes, *Studia Sci. Math. Hungar.* vol. 40, 2003, pp 243–256.

[11] G. Kéri and P.R.J. Östergård, Bounds for covering codes over large alphabets, *Designs, Codes and Cryptography*, vol. 137, 2005, pp 45–60.

[12] C. Mendes, E.L. Monte Carmelo, and M.V. Poggi de Aragão, Bounds for short covering codes and reactive tabu search, *Discrete Appl. Math.* vol 158, 2010, pp 522–533.

[13] E.L. Monte Carmelo, Covering codes arising from invariant sets under translation, unpublished.

[14] E.L. Monte Carmelo and C.F.X. De Mendonça Neto, Extremal problems on sum-free sets and coverings in tridimensional spaces, *Aequationes Mathematicae* vol. 78, 2009, pp 101-112.

[15] E.L. Monte Carmelo and I.N. Nakaoka, Short coverings in tridimensional spaces arising from sum-free sets, *European J. Combin.*, vol. 29, 2008, pp 227-233.

[16] E.L. Monte Carmelo, I.N. Nakaoka, and J.R. Gerônimo, A covering problem on finite spaces and rook domains, *Int. J. Appl. Math.*, vol. 20, 2007, pp 875–886.

[17] P.R.J. Östergård, *Construction methods for covering codes*, Helsinki University of Technology, Research Reports, 25. Espoo, Finland; 1993.

[18] P.R.J. Östergård, Upper bounds for q-ary covering codes, *IEEE Trans. Infor. Theory.*, vol 37(3), 1991, pp 660–664.

[19] P.R.J. Östergård and W.D. Weakley, Constructing covering codes with given automorphisms, *Des. Codes Cryptography,* vol 16, 1999, pp 65–73.

[20] O. Taussky and J. Todd, Covering theorems for groups, *Ann. Soc. Polonaise Math.* vol 21, 1948, pp 303–305.