Linear Algebra and its Applications 444 (2014) 42–52

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Invariant sets under linear operator and covering codes over modules

O.J.N.T.N. dos Santos [a], E.L. Monte Carmelo [b,1]

[a] *Universidade Estadual de Mato Grosso do Sul, Dourados, Brazil*
[b] *Departamento de Matemática, Universidade Estadual de Maringá, Brazil*

ARTICLE INFO

Article history:
Received 22 February 2013
Accepted 22 November 2013
Available online 12 December 2013
Submitted by R. Brualdi

MSC:
primary 94B65
secondary 13M99, 15A99, 11T71

Keywords:
Linear operator
Invariant set
Finite ring
Covering
Bound on code

ABSTRACT

Let A be a finite commutative ring with identity. A subset H of the A-module A^n is called an R-short covering of A^n if every vector of this module can be written as a sum of a scalar multiple of an element in H and an A-linear combination with at most R canonical vectors. Let $C(A,n,R)$ denote the smallest cardinality of an R-short covering of A^n. In order to explore the symmetries of such coverings, we investigate a characterization of invariant sets under certain linear operator over a finite ring A, based on its factorization into local rings. As a consequence, new classes of upper bounds on $C(A,n,R)$ are obtained, extending previous results. Moreover, an optimal class on $C(A,n,R)$ is derived from a construction of MDS codes over certain rings.

1. Introduction

Covering codes were posed by Taussky and Todd in 1948 from a group theoretical context in the seminal paper [18]. For our purpose, covering code is described when the alphabet A is a finite commutative ring with identity, and the space A^n is regarded as an A-module. A subset C of A^n is called an *R-covering* of A^n if every vector of A^n can be represented as a sum of a vector in C and an A-linear combination with at most R canonical vectors, that is, for each $v \in A^n$ there are $c \in C$ and scalars $\alpha_1, \dots, \alpha_R \in A$ such that

E-mail addresses: ojneto@uems.br (O.J.N.T.N. dos Santos), elmcarmelo@uem.br (E.L. Monte Carmelo).

[1] The author was partially supported by CNPq/MCT.

0024-3795/$ – see front matter
http://dx.doi.org/10.1016/j.laa.2013.11.034

$$v = c + \sum_{i=1}^{R} \alpha_i e_{j_i}, \tag{1}$$

where $\{e_1, \ldots, e_n\}$ represents the canonical base of A^n. Note that Eq. (1) means that the words v and c differ at most in R coordinates.

The minimum cardinality of an R-covering of A^n is denoted by $K_q(n, R)$, where A is an arbitrary ring with cardinality q. The determination of covering codes became a central problem in combinatorial coding theory due to a large number of connections with several branches of mathematics, computer science, information theory; motivated by applications to data transmission and storage systems. The literature on covering codes is so vast that many results are surveyed in [5]. Update tables on $K_q(n, R)$ are available in [9].

Several related extremal problems with algebraic constraints have been investigated, for instance, see the contributions [6,19]. In particular, a concept of covering is extended to an arbitrary module in [13], as described below. A subset H of A^n is called an R-*short covering* of A^n if each vector v in A^n can be written as

$$v = \alpha h + \sum_{i=1}^{R} \alpha_i e_{j_i}, \tag{2}$$

where $h \in H$ and $\alpha, \alpha_1, \ldots, \alpha_R \in A$. The induced number $C(A, n, R)$ denotes the smallest cardinality of an R-short covering of A^n.

As a numerical application, the new record-breaking $K_5(10, 7) = 9$ was derived from the value $C(\mathbb{Z}_5, 10, 7) = 2$. Moreover, the distinct behavior of short covering seems to be interesting on theoretical viewpoints. Indeed, connections with group theory, finite ring theory, combinatorial number theory, graph theory have been investigated, see [12] and its references. That work introduces a method for short covering based on invariant sets under linear operator in a vector space over a finite field.

As the main goal of this paper, we extend the method above to a module over an arbitrary finite ring. A characterization of invariant sets under certain linear operator is described by using a very-famous factorization of a finite ring into local rings. This generalization allows us to obtain new classes of upper bounds on $C(A, n, R)$ when A is a direct sum of finite fields, extending some previous results. This approach can be applied to classical covering too, improving a well-known upper bound by Östergård [15] under certain conditions. As the second goal, MDS codes over certain rings are investigated, extending a result by Carnielli [2]; thus new upper bounds on short coverings are derived as consequence.

This work is organized as follows. A few preliminary results are reported in Section 2, then we characterize short coverings with one element. The method based on invariant set under linear operator is extended to an arbitrary finite ring in Section 3. We investigate how this method produces several upper bounds on $C(A, n, R)$ and its impact on classical covering too. In Section 4, short coverings are constructed from MDS codes which are invariant by a suitable set of linear operators. New upper bounds and an exact class on short coverings are established. We conclude the work in Section 5 with a table of some new upper bounds.

2. Notation and preliminary results

It is worth stating that H is an R-short covering of A^n if and only if the set $A \cdot H = \{\alpha \cdot h\colon\ \alpha \in A \text{ and } h \in H\}$ is an R-covering of A^n. This remark allows us a systematic way to translate bounds, more precisely:

Proposition 2.1. *(See [13].) Let A be an arbitrary ring with q elements. For every $n > R \geqslant 1$,*

$$K_q(n, R) \leqslant (q - 1)C(A, n, R) + 1.$$