Linear Algebra and its Applications 524 (2017) 235–249

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Twisted centralizer codes

Adel Alahmadi [a], S.P. Glasby [b,c,*], Cheryl E. Praeger [a,b], Patrick Solé [d], Bahattin Yildiz [e]

[a] *Mathematics Department, King Abdulaziz University, Jeddah, Saudi Arabia*
[b] *Center for Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, WA 6009, Australia*
[c] *The Department of Mathematics, University of Canberra, ACT 2601, Australia*
[d] *CNRS/LAGA, University of Paris 8, 2 rue de la Liberté, 93 526 Saint-Denis, France*
[e] *University of Chester, UK*

A R T I C L E   I N F O

Article history:
Received 17 August 2016
Accepted 12 March 2017
Available online 16 March 2017
Submitted by R. Brualdi

MSC:
primary 94B05
secondary 13M05

Keywords:
Linear codes
Matrix codes
Minimal distance
Group centralizers

A B S T R A C T

Given an $n \times n$ matrix A over a field F and a scalar $a \in F$, we consider the linear codes $C(A, a) := \{B \in F^{n\times n} \mid AB = aBA\}$ of length n^2. We call $C(A, a)$ a *twisted centralizer code*. We investigate properties of these codes including their dimensions, minimum distances, parity-check matrices, syndromes, and automorphism groups. The minimal distance of a centralizer code (when $a = 1$) is at most n, however for $a \neq 0, 1$ the minimal distance can be much larger, as large as n^2.

Crown Copyright © 2017 Published by Elsevier Inc. All rights reserved.

* Corresponding author.
E-mail addresses: Stephen.Glasby@uwa.edu.au (S.P. Glasby), Cheryl.Praeger@uwa.edu.au (C.E. Praeger), sole@enst.fr (P. Solé), bahattinyildiz@gmail.com (B. Yildiz).

http://dx.doi.org/10.1016/j.laa.2017.03.011
0024-3795/Crown Copyright © 2017 Published by Elsevier Inc. All rights reserved.

1. Introduction

Denote the $n \times n$ matrices over a field F by $F^{n\times n}$. Fix a matrix $A \in F^{n\times n}$ and a scalar $a \in F$. As we are motivated by applications to coding theory we focus on the case where F is a finite field $\mathbb{F}_q$ of order q. The *centralizer of A, twisted by a,* is defined to be

$$C(A,a) := \{B \in F^{n\times n} \mid AB = aBA\}. \tag{1}$$

Clearly $C(A,a)$ is an F-linear subspace of the vector space $F^{n\times n}$. Note that $C(A,0)$ is the right-annihilator of A. We shall use the notation $C(A)$ instead of $C(A,1)$ when $a = 1$, and note that $C(A)$ is simply the centralizer of A. The subspace $C(A,a)$ of $F^{n\times n}$ is viewed as code: we view a codeword $B \in F^{n\times n}$ as column vector $[B]$ of length n^2, by reading the matrix B column-by-column. The case $a = 1$ was considered in [1]. In the present paper, we extend and sometimes correct the results of [1]. In particular the incorrect [1, Theorem 2.4] is corrected and generalized for this larger class of codes in [2] (see Theorem 2.3), and we exploit this result in several ways in Section 2.2.

Definition 1. For any $n\times n$ matrix $A \in F^{n\times n}$ and any scalar $a \in F$, the subspace $C(A,a)$ formed above is called the *centralizer code* obtained from A and *twisted by a*.

In a sense A serves as a parity-check matrix, because B lies in $C(A,a)$ precisely when $AB - aBA = 0$. More concretely, in the following result we show that a certain $n^2 \times n^2$ matrix H related to A is a parity check matrix in the sense that $B \in C(A,a)$ if and only if $H[B] = 0$, where $[B]$ is the n^2-dimensional column vector above corresponding to B.

Proposition 1.1. *A parity-check matrix for $C(A,a)$ is given by*

$$H = I_n \otimes A - a(A^t \otimes I_n),$$

where $\otimes$ denotes the Kronecker product, and A^t the transpose of the matrix A.

Proof. This follows from the proof of [10, Theorem 27.5.1, p. 124] with $A = A$, $B = aA$, $C = 0$. Also, a direct proof (for row vectors) is given in [2, Lemma 3.2]. □

The following simple observations involving $C(A,a)$ will be used later.

Theorem 1.2. *Suppose $a, a' \in F$ and $A \in F^{n\times n}$ is a matrix. Then the following are true:*

- **a)** *$A \in C(A,a)$ if and only if $a = 1$ or $A^2 = 0$.*
- **b)** *If $B \in C(A,a)$ and $B' \in C(A,a')$ then BB' and $B'B$ both lie in $C(A,aa')$.*
- **c)** *For $a \neq 0$, $B \in C(A,a) \Leftrightarrow A \in C(B,a^{-1})$.*

Download English Version:

https://daneshyari.com/en/article/5773055

Download Persian Version:

https://daneshyari.com/article/5773055

Daneshyari.com