Linear Algebra and its Applications 463 (2014) 68–77

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Centraliser codes

Adel Alahmadi [a], Shefa Alamoudi [a], Suat Karadeniz [b], Bahattin Yildiz [b], Cheryl Praeger [c], Patrick Solé [a,d,*]

[a] *Department of Mathematics, King Abdulaziz University, Jeddah, Saudi Arabia*
[b] *Department of Mathematics, Fatih University, 34500 Istanbul, Turkey*
[c] *Center for the Mathematics of Symmetry and Computation, School of Mathematics and Statistics, University of Western Australia, Perth, Australia*
[d] *Telecom ParisTech, France*

ARTICLE INFO

Article history:
Received 25 February 2014
Accepted 27 August 2014
Available online 16 September 2014
Submitted by R. Brualdi

MSC:
primary 94B05
secondary 13M05

Keywords:
Group centralisers
Matrix codes
Cyclic matrices
Separable matrices

ABSTRACT

Centraliser codes are codes of length n^2 defined as centralisers of a given matrix A of order n. Their dimension, parity-check matrices, syndromes, and automorphism groups are investigated. A lower bound on the dimension is n, the order of A. This bound is met when the minimal polynomial is equal to the annihilator, i.e. for so-called cyclic (a.k.a. non-derogatory) matrices. If, furthermore, the matrix is separable and the adjacency matrix of a graph, the automorphism group of that graph is shown to be abelian and to be even trivial if the alphabet field is of even characteristic.

1. Introduction

Let A be an $n \times n$ square matrix over some finite field $\mathbb{F}_q$. By $C(A)$ we mean the centraliser of A, namely:

* Corresponding author.
E-mail addresses: skaradeniz@fatih.edu.tr (S. Karadeniz), byildiz@fatih.edu.tr (B. Yildiz), sole@enst.fr (P. Solé).

http://dx.doi.org/10.1016/j.laa.2014.08.024
0024-3795/

$$C(A) := \{B \in \mathbb{F}_q^{n\times n} \mid AB = BA\}. \tag{1}$$

From basic linear algebra we know that $C(A)$ is a linear subspace of the vector space $\mathbb{F}_q^{n\times n}$ of all $n \times n$ matrices over $\mathbb{F}_q$. Now considering $C(A)$ as a subspace, we obtain a code whose elements are matrices, that can be viewed as vectors of length n^2, by reading them column by column.

Definition 1. For any q-ary $n \times n$ square matrix A, the subspace $C(A)$ formed above is called the **centraliser code** generated by A.

In a sense A serves as a parity-check matrix as well, because for any $n \times n$ matrix $B \in \mathbb{F}_q^{n\times n}$, we have

$$B \in C(A) \quad \Leftrightarrow \quad AB - BA = 0.$$

More concretely, we have the following result.

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

$$H = I_n \otimes A - \left(A^T \otimes I_n\right),$$

with $\otimes$ denoting the Kronecker product, and M^T the transpose of the matrix M.

Proof. Consider the map $B \mapsto AB$. If we think of B as written off column by column into a vector of length n^2, say $Vec(B)$, then the matrix of this map is readily seen to be $I_n \otimes A$. Thus $Vec(AB) = (I_n \otimes A)\ Vec(B)$. Let T_n be the $n^2 \times n^2$ matrix of the endomorphism $B \mapsto B^T$, that is $Vec(B^T) = T_n\ Vec(B)$. By a similar calculation the matrix of the map $B \mapsto BA = (A^T B^T)^T$, turns out to be, after some algebra, $T_n(I_n \otimes A^T)T_n$. The result follows now upon applying the identity

$$T_n\left(A' \otimes B'\right)T_n = \left(B' \otimes A'\right)$$

of [3, Corollary 52, p. 44] in the special case $A' = I_n$, $B' = A^T$. □

The problems about $C(A)$ that arise naturally for a given A include

- computing its dimension
- finding efficient encoding and decoding procedures
- determining its automorphism group

The paper is organized as follows. Sections 2, 3, 4 tackle in order the above three problems. Section 5 is dedicated to concrete examples of codes and Section 6 contains some concluding remarks and open problems.