Finite Fields and Their Applications 40 (2016) 224–245

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A characterization of MDS codes that have an error correcting pair

Irene Márquez-Corbella [a,*], Ruud Pellikaan [b,*]

[a] *INRIA Paris, 2 rue Simone Iff, CS 42112, 75589 Paris Cedex 12, France*
[b] *Department of Mathematics and Computing Science, Eindhoven University of Technology, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*

ARTICLE INFO

Article history:
Received 12 August 2015
Received in revised form 29 February 2016
Accepted 21 April 2016
Available online 10 May 2016
Communicated by Pascale Charpin

MSC:
14G50
11T71
94B

Keywords:
Error–correcting pairs
MDS codes
GRS codes

ABSTRACT

Error–correcting pairs were introduced in 1988 in the preprint [1] that appeared in [2], and were found independently in [3], as a general algebraic method of decoding linear codes. These pairs exist for several classes of codes. However little or no study has been made for characterizing those codes. This article is an attempt to fill the vacuum left by the literature concerning this subject. Since every linear code is contained in an MDS code of the same minimum distance over some finite field extension, see [4], we have focused our study on the class of MDS codes. Our main result states that an MDS code of minimum distance $2t+1$ has a t-ECP if and only if it is a generalized Reed–Solomon (GRS) code. A second proof is given using recent results [5,6] on the Schur product of codes.

* Corresponding authors.
E-mail addresses: irene.marquez-corbella@inria.fr (I. Márquez-Corbella), g.r.pellikaan@tue.nl (R. Pellikaan).
URLs: http://www.singacom.uva.es/~iremarquez (I. Márquez-Corbella), http://www.win.tue.nl/~ruudp/ (R. Pellikaan).

http://dx.doi.org/10.1016/j.ffa.2016.04.004
1071-5797/

1. Introduction

Error–correcting pairs were introduced in [1,2], and independently in [3], as a general algebraic method of decoding linear codes. These pairs exist for several classes of codes such as for generalized Reed–Solomon (RS), cyclic, alternant and algebraic geometry codes [7,8,3,9,10,2,4]. The aim of this paper is to characterize those MDS codes that have a t-error correcting pair. This was shown for $t \leq 2$ in [4].

Section 2 gives the background of MDS codes. Generalized Reed–Solomon (GRS) codes and an equivalent way to describe such a code as a projective system on a rational normal curve in projective space are reviewed in Section 3. We give here also a survey of well-known results related to GRS codes which are used to set the notation and to recall some properties that are relevant for the proof of the main result. Moreover, a classical result is stated: a rational curve in projective r space is uniquely determined by n of its points in case $n \geq r + 2$. This classical result will be vital in our main result (see Appendix D).

For further details on the notion of an error correcting pair see Section 4 where we formally review this definition, detailing the state-of-art and the existence of error correcting pairs for some families of codes.

Section 5 gives a brief exposition of classical methods of constructing a shorter code out of a given one: the process of puncturing and shortening a code. In particular we will be concerned with the case of these operations for MDS codes.

Finally, in Section 6 we present the main result of this paper that states that every MDS code with minimum distance $2t + 1$ that has a t-ECP belongs to the class of GRS codes. In Section 7 we extend recent results on the Schur product of codes [6,5] to give an independent proof of our main result.

1.1. Notation

By $\mathbb{F}_q$ where q is a prime power, we denote a finite field with q elements. The projective line over the finite field $\mathbb{F}_q$, denoted by $\mathbb{P}^1(\mathbb{F}_q)$, is the set $\mathbb{F}_q \cup \{\infty\}$, and $\mathbb{F}_q^*$ denotes the set of units of $\mathbb{F}_q$.

An $[n, k]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. We will denote the length of C by $n(C)$, its dimension by $k(C)$ and its minimum distance by $d(C)$.

Given two elements $\mathbf{a}$ and $\mathbf{b}$ on $\mathbb{F}_q^n$ the *star multiplication* is defined by coordinatewise multiplication, that is $\mathbf{a} * \mathbf{b} = (a_1 b_1, \ldots, a_n b_n)$. Let A and B be two codes in $\mathbb{F}_q^n$. Then, $A * B$ is the code in $\mathbb{F}_q^n$ generated by $\{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B\}$. Note that, in this paper, $A * B$ is not the set $\{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in A \text{ and } \mathbf{b} \in B\}$ as in [2], but the space generated by that set.

The *standard inner multiplication* is defined by $\mathbf{a} \cdot \mathbf{b} = \sum_{i=1}^{n} a_i b_i$ of $\mathbf{a}$ and $\mathbf{b}$ on $\mathbb{F}_q^n$. Now $A \perp B$ if and only if $\mathbf{a} \cdot \mathbf{b} = 0$ for all $\mathbf{a} \in A$ and $\mathbf{b} \in B$.