Finite Fields and Their Applications 37 (2016) 85–107

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Projective Reed–Muller type codes on rational normal scrolls

Cícero Carvalho [*,1], Victor G.L. Neumann [2]

Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J. N. Ávila 2121, 38.408-902 Uberlândia, MG, Brazil

A R T I C L E   I N F O

Article history:
Received 30 April 2014
Received in revised form 10 July 2015
Accepted 11 September 2015
Available online 26 September 2015
Communicated by Xiang-dong Hou

MSC:
11T71
13P25
94B60

Keywords:
Projective variety codes
Evaluation codes
Reed–Muller type codes
Gröbner bases

A B S T R A C T

In this paper we study an instance of projective Reed–Muller type codes, i.e., codes obtained by the evaluation of homogeneous polynomials of a fixed degree in the points of a projective variety. In our case the variety is an important example of a determinantal variety, namely the projective surface known as rational normal scroll, defined over a finite field, which is the basic underlining algebraic structure of this work. We determine the dimension and a lower bound for the minimum distance of the codes, and in many cases we also find the exact value of the minimum distance. To obtain the results we use some methods from Gröbner bases theory.

* Corresponding author.
E-mail addresses: cicero@ufu.br (C. Carvalho), gonzalo@famat.ufu.br (V.G.L. Neumann).

[1] Partially supported by CNPq (proc. 302280/2011-1 and 480477/2013-2) and FAPEMIG.
[2] Partially supported by CNPq (proc. 480477/2013-2) and FAPEMIG.

http://dx.doi.org/10.1016/j.ffa.2015.09.004
1071-5797/

1. Introduction

Since the construction of algebraic geometry codes by V.D. Goppa (see [2]) in 1983, concepts and tools from algebraic geometry, as well as from commutative algebra, have become increasingly important in coding theory. The codes produced using Goppa construction may be thought of as a particular case of the so-called evaluation codes, meaning that functions from a certain vector space are evaluated on points of an algebraic variety, or more generally, on a set of points of an affine or projective space over $\mathbb{F}_q$, a finite field with q elements.

In 1991 Sørensen determined the parameters of the projective Reed–Muller codes, obtained by evaluating all homogeneous polynomials of degree d in $\mathbb{F}_q[X_0, \dots, X_n]$ at the points of $\mathbb{P}^n(\mathbb{F}_q)$ thus obtaining a code in $\mathbb{F}_q^m$, where $m = \#(\mathbb{P}^n(\mathbb{F}_q)) = (q^n-1)/(q-1)$ (see [7]). For the purpose of the evaluation the coordinates of the points in the projective space are considered to be in the standard notation, i.e. the leftmost nonzero entry is 1. Since then many other projective evaluation codes have been studied, where one replaces $\mathbb{P}^n(\mathbb{F}_q)$ by e.g. a zero-dimensional complete intersection in $\mathbb{P}^n(\mathbb{F}_q)$ (see [5]), the Segre variety (see [6]), smooth quadric surfaces and twisted Segre varieties (see [4]), etc.

In this paper we study the projective evaluation codes obtained by evaluating homogeneous polynomials of degree d at the points of a rational normal scroll, a projective surface which we define as follows.

Definition 1.1. Let m and n be integers such that $1 \le m \le n$ and let $l = n + m + 1$. A rational normal scroll $S \subset \mathbb{P}^l(\mathbb{F}_q)$ is the algebraic surface defined by

$$S = \left\{ (x_0 : \cdots : x_l) \in \mathbb{P}^l(\mathbb{F}_q) \mid \operatorname{rank} \begin{pmatrix} x_0 & \cdots & x_{n-1} & x_{n+1} & \cdots & x_{l-1} \\ x_1 & \cdots & x_n & x_{n+2} & \cdots & x_l \end{pmatrix} = 1 \right\} .$$

Let S_0 be the open subset of S isomorphic to the affine plane given by

$$S_0 = \left\{ (1 : a : \cdots : a^n : b : ab : \cdots : a^m b) \mid (a, b) \in \mathbb{A}^2(\mathbb{F}_q) \right\} ,$$

and let C_∞ and L_∞ be the rational curves on S given by

$$C_\infty = \left\{ (0 : \cdots : 0 : a_0^m : a_0^{m-1} a_1 : \cdots : a_1^m) \in S \mid (a_0 : a_1) \in \mathbb{P}^1(\mathbb{F}_q) \right\} \text{ and}$$
$$L_\infty = \left\{ (0 : \cdots : 0 : \lambda : 0 : \cdots : 0 : \mu) \in S \mid (\lambda : \mu) \in \mathbb{P}^1(\mathbb{F}_q) \right\} .$$

It is not difficult to check that $S = S_0 \cup L_\infty \cup C_\infty$ (see e.g. [3, Section 1]) where the union is disjoint, except for the point at the intersection of the two rational curves, thus S has

$$N = q^2 + 2(q + 1) - 1 = (q + 1)^2$$