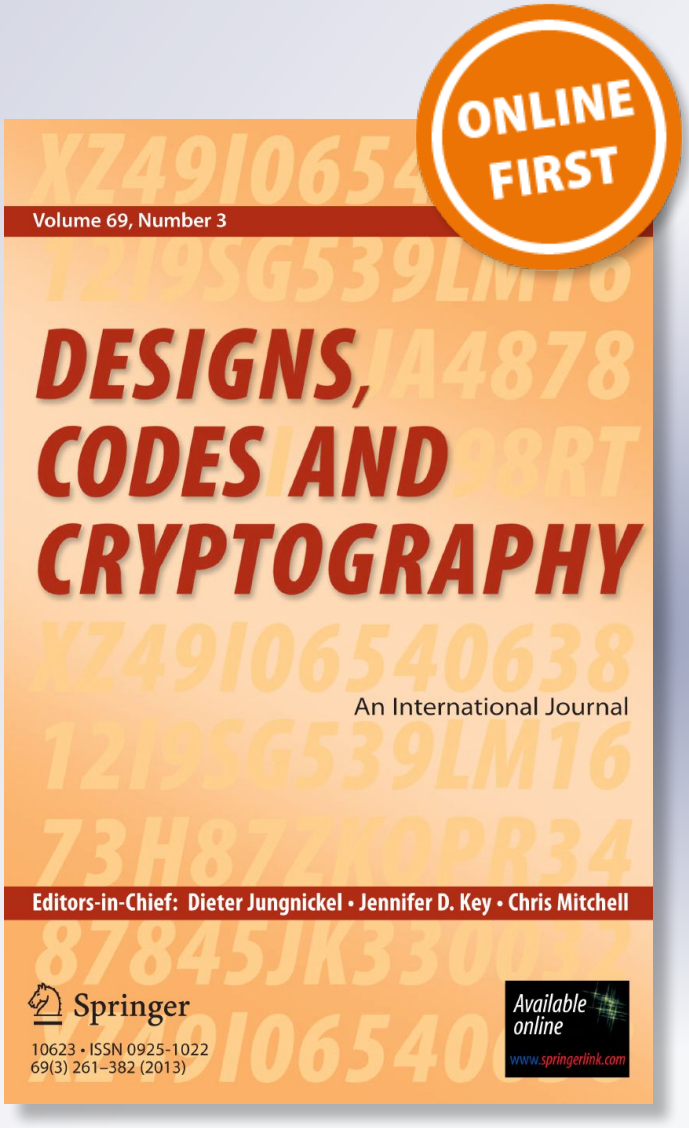
Projective Reed–Muller type codes on higher dimensional scrolls

Cícero Carvalho, Xavier Ramírez-Mondragón, Victor G. L. Neumann & Horacio Tapia-Recillas

Designs, Codes and Cryptography
An International Journal

ISSN 0925-1022

Des. Codes Cryptogr.
DOI 10.1007/s10623-018-00603-8



Springer

Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-018-00603-8

Projective Reed–Muller type codes on higher dimensional scrolls

Cícero Carvalho[1] · **Xavier Ramírez-Mondragón**[2] · **Victor G. L. Neumann**[1] · **Horacio Tapia-Recillas**[2]

Received: 2 November 2017 / Revised: 12 November 2018 / Accepted: 20 December 2018

Abstract
In 1988 Lachaud introduced the class of projective Reed–Muller codes, defined by evaluating the space of homogeneous polynomials of a fixed degree d on the points of $\mathbb{P}^n(\mathbb{F}_q)$. In this paper we evaluate the same space of polynomials on the points of a higher dimensional scroll, defined from a set of rational normal curves contained in complementary linear subspaces of a projective space. We determine a formula for the dimension of the codes, and the exact value of the dimension and the minimum distance in some special cases.

Keywords Projective variety codes · Evaluation codes · Reed–Muller type codes · Higher dimensional scroll

Mathematics Subject Classification 11T71 · 13P25 · 94B60

Communicated by G. Korchmaros.

C. Carvalho and V. G. L. Neumann are partially supported by CNPq and FAPEMIG. X. Ramírez-Mondragón is supported by CONACyT Scholarship No. 209918.

✉ Xavier Ramírez-Mondragón
xavierrmondragon@gmail.com

Cícero Carvalho
cicero@ufu.br

Victor G. L. Neumann
victor.neumann@ufu.br

Horacio Tapia-Recillas
htr@xanum.uam.mx

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

[2] Departamento de Matemáticas, Universidad Autónoma Metropolitana, Av. San Rafael Atlixco 186, Col. Vicentina, C.P. 09340, Delegación Iztapalapa, CD. Mexico, Mexico

Published online: 05 January 2019

1 Introduction

In 1988 Lachaud introduced the class of projective Reed–Muller codes (see [14]), defined by evaluating the space of homogeneous polynomials of a fixed degree d on the points of $\mathbb{P}^n(\mathbb{F}_q)$, the n-dimensional projective space over a finite field $\mathbb{F}_q$ with q elements. For the purpose of the evaluation, the coordinates of the points in the projective space are considered to be written in *standard notation*, i.e., the leftmost nonzero entry is equal to 1. In [17] Sörensen found formulas for the dimension and minimum distance of these codes and in [15] Rentería and Tapia-Recillas gave a different approach to arrive at those formulas. Recently, there has been some interest in the problem of determining the generalized Hamming weights of projective Reed–Muller type codes (see [2,3,10]).

The classical definition of the projective Reed–Muller code can be extended to arbitrary subsets $\mathcal{X}$ of the projective space $\mathbb{P}^n(\mathbb{F}_q)$, and the codes thus produced are called Reed–Muller type (projective) codes. Several instances where $\mathcal{X}$ is the set of $\mathbb{F}_q$-rational points of a projective variety defined over $\mathbb{F}_q$ have already been studied, for example, the cases where $\mathcal{X}$ is a zero-dimensional complete intersection in $\mathbb{P}^n(\mathbb{F}_q)$ [9], the Segre variety [11], smooth quadric surfaces and twisted Segre varieties [7], and the Veronese variety [16], among others (see [5,6,12,15]). These investigations form a growing corpus of theoretical knowledge which is crucial for future applications. Of course, they must be paired with studies on the decoding of the proposed codes. Also, for practical applications, a code may have to wait for the right moment, for example, Reed-Solomon codes were created in 1960 but started to be widely used in applications only in the beginning of the 80's, with the appearance of CD's.

In the present manuscript we continue the study of projective Reed–Muller type codes set forward by the above works. In [5] the authors studied the case where $\mathcal{X}$ is a rational normal scroll surface. They determined the dimension of the codes, a lower bound for the minimum distance and its exact value in some cases. In this paper we consider higher dimensional scrolls, defined from a set of rational normal curves contained in complementary linear subspaces of a projective space. We also determine a formula for the dimension of the codes, and the exact value of the dimension and the minimum distance in some special cases. To prove our results we generalized some of the methods used in [5], and we present them in a more systematic form. A relationship between the introduced codes and a direct product of (classical) projective Reed–Muller codes is given, which explains the formula for the exact value of the minimum distance in some cases.

The paper is organized as follows. In the next section, the higher dimensional scroll S (following [13]) over the finite field $\mathbb{F}_q$ and the projective Reed–Muller type code $C_S(d)$ obtained by evaluating homogeneous polynomials of degree d at its $\mathbb{F}_q$-rational points are introduced. In Sect. 3, an alternative construction for $C_S(d)$, which will be of fundamental importance in the determination of its parameters is presented. Then, we proceed to determine a general formula for the dimension of $C_S(d)$ and its exact value in particular cases. Examples of the studied codes are given where the parameters are completely determined. In the last section, a connection between a special case of $C_S(d)$ and the direct product of (classical) projective Reed–Muller codes is presented, which allows the determination of the parameters of $C_S(d)$.

2 Higher dimensional scrolls and Reed–Muller type codes

In this section we present the definition of higher dimensional scrolls and the codes which we will study in the rest of the manuscript. We refer the interested reader to [13] for results and concepts on algebraic geometry, particularly in higher dimensional scrolls.

Let $e \geq 1$ be an integer. *A rational normal curve of degree e* is the image of the map

$$\begin{aligned} v_e \colon \mathbb{P}^1(\mathbb{F}_q) &\to \mathbb{P}^e(\mathbb{F}_q) \\ (x_0 : x_1) &\mapsto (x_0^e : x_0^{e-1}x_1 : \cdots : x_1^e). \end{aligned}$$

Let $e_0 \geq e_1 \geq e_2 \geq \ldots \geq e_n \geq 1$ be integers, and let

$$\ell = (e_0 + 1) + (e_1 + 1) + \cdots + (e_n + 1) - 1 = \sum_{i=0}^{n} e_i + n.$$

A point in $\mathbb{P}^\ell(\mathbb{F}_q)$ will be denoted by

$$\left(x_{0,0} : \cdots : x_{0,e_0} : x_{1,0} : \cdots : x_{1,e_1} : \cdots : x_{n,0} : \cdots : x_{n,e_n}\right).$$

For $i \in \{0, \ldots, n\}$, the set of points in $\mathbb{P}^\ell(\mathbb{F}_q)$ such that $x_{s,t} = 0$ for all $t \in \{0, \ldots, e_s\}$ and all $s \in \{0, \ldots, n\}\backslash\{i\}$ is a linear subspace of dimension e_i, which is denoted by $\mathbf{P}^{e_i}$, and the image of the map

$$\begin{aligned} u_i \colon \mathbb{P}^1(\mathbb{F}_q) &\to \mathbf{P}^{e_i} \subset \mathbb{P}^\ell(\mathbb{F}_q) \\ (b_0 : b_1) &\mapsto \left(0 : \cdots : b_0^{e_i} : b_0^{e_i-1}b_1 : \cdots : b_1^{e_i} : 0 \cdots : 0\right), \end{aligned}$$

is a rational normal curve of degree e_i. For each $(b_0 : b_1) \in \mathbb{P}^1(\mathbb{F}_q)$, we define $L_{(b_0:b_1)}$ as the linear subspace of $\mathbb{P}^\ell(\mathbb{F}_q)$ spanned by the points $u_0(b_0 : b_1), \ldots, u_n(b_0 : b_1)$, i.e., $L_{(b_0:b_1)}$ is the set of points of the form

$$\left(a_0 b_0^{e_0} : a_0 b_0^{e_0-1} b_1 : \cdots : a_0 b_1^{e_0} : \cdots : a_n b_0^{e_n} : a_n b_0^{e_n-1} b_1 : \cdots : a_n b_1^{e_n}\right),$$

where $(a_0 : \cdots : a_n) \in \mathbb{P}^n(\mathbb{F}_q)$.

Definition 2.1 The higher dimensional scroll of type $e_0, \ldots, e_n$ is the set

$$S_{e_0,\ldots,e_n} := \bigcup_{(b_0:b_1)\in\mathbb{P}^1} L_{(b_0:b_1)} \subset \mathbb{P}^\ell(\mathbb{F}_q).$$

If $n = 1$ the previous definition gives the rational normal scroll studied in [5] and in this work some results presented there are generalized.

From now on, we will only write scroll when we refer to a higher dimensional scroll. Everything we did so far in this section makes sense if we replace $\mathbb{F}_q$ by any field K. If K is an algebraically closed field it is shown that $S_{e_0,\ldots,e_n}$ is an algebraic variety of dimension $n + 1$ which is the zero locus in $\mathbb{P}^\ell(K)$ of the ideal of polynomials in $K[X_{0,0}, \ldots, X_{0,e_0}, \ldots, X_{n,0}, \ldots, X_{n,e_n}]$ generated by the 2×2 minors of the $2 \times (l + 1)$ matrix (see for instance pp. 92–93 and 105–109 of [13]),

$$\mathcal{M} = \begin{pmatrix} X_{0,0} & \ldots & X_{0,e_0-1} & X_{1,0} & \ldots & X_{1,e_1-1} & \ldots & X_{n,0} & \ldots & X_{n,e_n-1} \\ X_{0,1} & \ldots & X_{0,e_0} & X_{1,1} & \ldots & X_{1,e_1} & \ldots & X_{n,1} & \ldots & X_{n,e_n} \end{pmatrix}.$$

Since the integers $e_0, \ldots, e_n$ are fixed throughout the paper, below we will denote $S_{e_0,\ldots,e_n}$ simply by S. In [5] the authors use the fact that the rational normal scroll surface is a disjoint union of lines. Here a generalization of this result is given which will be used to count the number of rational points of S.

Proposition 2.2 *If $(b_0 : b_1)$ and $(\tilde{b}_0 : \tilde{b}_1)$ are distinct points of $\mathbb{P}^1(\mathbb{F}_q)$ then $L_{(b_0:b_1)}$ and $L_{(\tilde{b}_0:\tilde{b}_1)}$ are disjoint subspaces.*

Proof Suppose $(a_0 : \cdots : a_n)$ and $(\tilde{a}_0 : \cdots : \tilde{a}_n)$ exists in $\mathbb{P}^n(\mathbb{F}_q)$ such that

$$\begin{aligned}&\left(a_0 b_0^{e_0} : a_0 b_0^{e_0-1} b_1 : \cdots : a_0 b_1^{e_0} : \cdots : a_n b_0^{e_n} : a_n b_0^{e_n-1} b_1 : \cdots : a_n b_1^{e_n}\right)\\ &\quad = \left(\tilde{a}_0 \tilde{b}_0^{e_0} : \tilde{a}_0 \tilde{b}_0^{e_0-1} \tilde{b}_1 : \cdots : \tilde{a}_0 \tilde{b}_1^{e_0} : \cdots : \tilde{a}_n \tilde{b}_0^{e_n} : \tilde{a}_n \tilde{b}_0^{e_n-1} \tilde{b}_1 : \cdots : \tilde{a}_n \tilde{b}_1^{e_n}\right).\end{aligned}$$

Let j be the least subscript for which $a_j \neq 0$. Assume that $b_0 \neq 0$, then the first nonzero entry from left to right in the coordinates of the common point is $a_j b_0^{e_j}$, at position $(j, 0)$, so in particular, for all $i < j$ we have $\tilde{a}_i \tilde{b}_0^{e_i} = 0$ and so $\tilde{a}_i = 0$. Also, we must have $\tilde{a}_j \tilde{b}_0^{e_j} \neq 0$ so that $\tilde{a}_j \neq 0$. Taking the ratios between entry $(j, 1)$ and $(j, 0)$ we get

$$\frac{a_j b_0^{e_j-1} b_1}{a_j b_0^{e_j}} = \frac{\tilde{a}_j \tilde{b}_0^{e_j-1} \tilde{b}_1}{\tilde{a}_j \tilde{b}_0^{e_j}},$$

hence $b_1/b_0 = \tilde{b}_1/\tilde{b}_0$.

Now assume that $b_0 = 0$, then the first nonzero entry from left to right in the coordinates of the common point is $a_j b_1^{e_j}$, at position (j, e_j), hence $\tilde{a}_j \tilde{b}_1^{e_j} \neq 0$ and for all $i < j$ we have $\tilde{a}_i \tilde{b}_1^{e_j} = 0$, so that $\tilde{a}_i = 0$. We also have $\tilde{a}_j \tilde{b}_0^{e_j} = 0$, hence $\tilde{b}_0 = 0$. This concludes the proof that we must have $(b_0 : b_1) = (\tilde{b}_0 : \tilde{b}_1)$. □

Corollary 2.3 *S is the disjoint union of $q + 1$ linear subspaces of dimension n and $|S| = (q^n + \cdots + q + 1)(q + 1)$.*

Proof For any $(b_0 : b_1) \in \mathbb{P}^1(\mathbb{F}_q)$ the points in the set $\{u_0(b_0 : b_1), \ldots, u_n(b_0 : b_1)\}$ lie in linear subspaces of $\mathbb{P}^\ell(\mathbb{F}_q)$ which are mutually disjoint, thus the set is linearly independent and $L_{(b_0:b_1)}$ is a linear space of dimension n. Consequently $L_{(b_0:b_1)}$ contains $q^n + \cdots + q + 1$ rational points and hence $|S| = (q^n + \cdots + q + 1)(q + 1)$. □

Let $N := (q^n + \cdots + q + 1)(q + 1)$ and let $P_1, \ldots, P_N$ be the rational points of the scroll. We write

$$\mathbb{F}_q[\mathbf{X}] := \mathbb{F}_q\left[X_{0,0}, \ldots, X_{0,e_0}, X_{1,0}, \ldots, X_{1,e_1}, \ldots, X_{n,0}, \ldots, X_{n,e_n}\right],$$

and for a nonnegative integer d, $\mathbb{F}_q[\mathbf{X}]_d$, will denote the $\mathbb{F}_q$-vector space of polynomials in $\mathbb{F}_q[\mathbf{X}]$ of degree d.

Definition 2.4 Let

$$\begin{aligned} ev_d : \mathbb{F}_q[\mathbf{X}]_d &\to \mathbb{F}_q^N \\ f &\mapsto (f(P_1), \ldots, f(P_N)) \end{aligned}$$

be the evaluation morphism, where the (rational) points of the scroll are written in standard notation. Clearly ev_d is an $\mathbb{F}_q$-linear transformation and its image, denoted by $C_S(d)$, is the *projective Reed–Muller type code associated to S*.

Let I_S be the ideal of $\mathbb{F}_q[\mathbf{X}]$ generated by all homogeneous polynomials which vanish on S and denote by $I_S(d)$ its degree d component, then clearly $C_S(d)$ is isomorphic, as an $\mathbb{F}_q$-vector space, to $\mathbb{F}_q[\mathbf{X}]_d / I_S(d)$.

We endow the set of monomials in $\mathbb{F}_q[\mathbf{X}]$ with the lexicographic order where

$$X_{0,0} > X_{0,1} > \cdots > X_{0,e_0} > X_{1,1} > \cdots > X_{1,e_1} > \cdots > X_{n,0} > \cdots > X_{n,e_n}.$$

For $s, u \in \{0, \ldots, n\}$, $t \in \{0, \ldots, e_s - 1\}$, $v \in \{1, \ldots, e_u\}$ with either $s < u$ or $s = u$ and $t + 1 < v$, let

$$g_{(s,t),(u,v)} := X_{s,t}X_{u,v} - X_{s,t+1}X_{u,v-1}.$$

Let G be the set of all polynomials $g_{(s,t),(u,v)}$ which are the 2×2 minors of the matrix $\mathcal{M}$ introduced above, and let I denote the ideal of $\mathbb{F}_q[\mathbf{X}]$ generated by G. Clearly $I \subset I_S$. It will be shown that $I \subsetneq I_S$, and the following result is needed in order to do so.

Proposition 2.5 *The set G is a Gröbner basis for I.*

Proof Let $g_{(s,t),(u,v)}, g_{(i,j),(k,l)} \in G$ and observe that their leading monomials are $X_{s,t}X_{u,v}$ and $X_{i,j}X_{k,l}$, respectively. According to [8, pp. 103–104], in order to prove that G is a Gröbner basis for I it suffices to show that the S-polynomial of $g_{(s,t),(u,v)}$ and $g_{(i,j),(k,l)}$, in the case where the leading monomials are not coprime, may be written as $a_1g_1 + \cdots + a_mg_m$, with $a_i \in \mathbb{F}_q[\mathbf{X}]$, $g_i \in G$ and the leading monomial of a_ig_i being less or equal to the leading monomial of the S-polynomial, for all $i = 1, \ldots, m$.

Assume that $X_{s,t} < X_{i,j}$. Then we must have either $X_{u,v} = X_{i,j}$ or $X_{u,v} = X_{k,l}$ so that $X_{s,t}X_{u,v}$ and $X_{i,j}X_{k,l}$ are not coprime. If $X_{u,v} = X_{i,j}$, then

$$\begin{aligned} S(g_{(s,t),(u,v)}, g_{(u,v),(k,l)}) &= X_{k,l}\ g_{(s,t),(u,v)} - X_{s,t}\ g_{(u,v),(k,l)} \\ &= -X_{k,l}X_{s,t+1}X_{u,v-1} + X_{s,t}X_{u,v+1}X_{k,l-1} \\ &= -X_{s,t+1}(X_{u,v-1}X_{k,l} - X_{u,v}X_{k,l-1}) \\ &\quad + X_{k,l-1}(X_{s,t}X_{u,v+1} - X_{s,t+1}X_{u,v}) \\ &= -X_{s,t+1}g_{(u,v-1),(k,l)} + X_{k,l-1}g_{(s,t),(u,v+1)}. \end{aligned}$$

If $X_{u,v} = X_{k,l}$, then

$$\begin{aligned} S(g_{(s,t),(u,v)}, g_{(i,j),(u,v)}) &= X_{i,j}\ g_{(s,t),(u,v)} - X_{s,t}\ g_{(i,j),(u,v)} \\ &= X_{s,t}X_{i,j+1}X_{u,v-1} - X_{i,j}X_{s,t+1}X_{u,v-1} \\ &= X_{u,v-1}g_{(s,t),(i,j+1)}. \end{aligned}$$

Assume now that $X_{s,t} = X_{i,j}$ (and assume w.l.g. that $X_{u,v} > X_{k,l}$). Then

$$S(g_{(s,t),(u,v)}, g_{(s,t),(k,l)}) = -X_{s,t+1}(X_{u,v-1}X_{k,l} - X_{u,v}X_{k,l-1}).$$

Since $X_{u,v} > X_{k,l}$, it follows that either $u < k$ or $u = k$ and $v < l$, so in either case $S(g_{(s,t),(u,v)}, g_{(s,t),(k,l)}) = -X_{s,t+1}g_{(u,v-1),(k,l)}$. This concludes the proof of the Proposition. □

A consequence of this Proposition is that $I \subsetneq I_S$. Indeed, consider the polynomial $X_{0,0}^qX_{1,0} - X_{0,0}X_{1,0}^q$ which clearly vanishes at all points of $\mathbb{P}^\ell(\mathbb{F}_q)$. Its leading monomial is $X_{0,0}^qX_{1,0}$ and (since $X_{0,0}$ and $X_{1,0}$ only appear in the first row of $\mathcal{M}$) one can easily check that it is not a multiple of the leading monomial of any polynomial in G, hence it is not an element of I.

3 An alternative construction of $C_S(d)$

As observed above, the ideal I_S contains properly the ideal I, and as far as we can tell, it is not easily determined. Instead of determining I_S, or $I_S(d)$ directly, we follow the ideas (and

generalize the methods) of [5] to find a quotient which is isomorphic to $\mathbb{F}_q[\mathbf{X}]_d/I_S(d)$, to compute the dimension of $C_S(d)$.

Motivated by the construction of the higher dimensional scroll, and the expression of the entries of the points in the spaces $L_{(b_0:b_1)}$, we define the following morphism of algebras

$$\psi : \mathbb{F}_q[\mathbf{X}] \to \mathbb{F}_q[Y_0, \ldots, Y_n, Z_0, Z_1],$$

which takes $X_{i,j}$ to $Y_i Z_0^{e_i-j} Z_1^j$ for all $i \in \{0, \ldots, n\}$ and $j \in \{0, \ldots, e_i\}$.

We will write $\mathbb{F}_q[\mathbf{Y}, \mathbf{Z}]$ for $\mathbb{F}_q[Y_0, \ldots, Y_n, Z_0, Z_1]$. The following Lemma, whose (omitted) proof consists of simple calculations, shows what the image under ψ of a monomial looks like.

Lemma 3.1 *Let $X_{0,0}^{\alpha_{0,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}} \in \mathbb{F}_q[\mathbf{X}]_d$ be a monomial of degree d and let $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ be its image under ψ. Then:*

1. $\beta_i = \sum_{j=0}^{e_i} \alpha_{i,j}$ *for all* $0 \le i \le n$.
2. $\sum_{i=0}^{n} \beta_i = d$.
3. $\gamma_0 = \sum_{i=0}^{n} \sum_{j=0}^{e_i} (e_i - j)\alpha_{i,j}$.
4. $\gamma_1 = \sum_{i=0}^{n} \sum_{j=0}^{e_i} j\alpha_{i,j}$.
5. $\gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i \beta_i$.

Let $\mathcal{B} := \psi(\mathbb{F}_q[\mathbf{X}]) \subset \mathbb{F}_q[\mathbf{Y}, \mathbf{Z}]$. Then $\mathcal{B}$ has the graded algebra structure by taking the degree of $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ as $\sum_{i=0}^{n} \beta_i$. Thus its homogeneous component of degree d, $\mathcal{B}_d$, is $\psi(\mathbb{F}_q[\mathbf{X}]_d)$ and ψ is a (degree zero) morphism of graded algebras.

Proposition 3.2 *$\mathcal{B}_d$ is a finite $\mathbb{F}_q$-vector space which has*

$$M_d := \left\{ Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \mathbb{F}_q[\mathbf{Y}, \mathbf{Z}] : \sum_{i=0}^{n} \beta_i = d, \gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i \beta_i \right\}$$

as a basis.

Proof From the above Lemma it follows that $\mathcal{B}_d$ is a subspace of the space generated by M_d. To show the other inclusion, let $\beta_0, \ldots, \beta_n$ be nonnegative integers such that $\sum_{i=0}^{n} \beta_i = d$. It suffices to prove that any monomial of the form $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$, with $\gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i \beta_i$, is an element of $\mathcal{B}_d$, and for this we will do an induction on γ_0.

When $\gamma_0 = 0$ we have

$$\psi\left(X_{0,e_0}^{\beta_0} X_{1,e_1}^{\beta_1} \cdots X_{n,e_n}^{\beta_n}\right) = Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^0 Z_1^{\sum_{i=0}^{n} e_i \beta_i} \in \mathcal{B}_d.$$

Now assume that given $0 \le \gamma_0 < \sum_{i=0}^{n} e_i \beta_i$ and nonnegative integers $\beta_0, \ldots, \beta_n$ such that $\sum_{i=0}^{n} \beta_i = d$, a monomial exists

$$X_{0,0}^{\alpha_{0,0}} \cdots X_{0,e_0}^{\alpha_{0,e_0}} \cdots X_{n,0}^{\alpha_{n,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}},$$

such that

$$\psi\left(X_{0,0}^{\alpha_{0,0}} \cdots X_{0,e_0}^{\alpha_{0,e_0}} \cdots X_{n,0}^{\alpha_{n,0}} \cdots X_{n,e_n}^{\alpha_{n,e_n}}\right) = Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1},$$

where $\gamma_0 + \gamma_1 = \sum_{i=0}^{n} e_i \beta_i$. Note that $\gamma_1 > 0$ so $\alpha_{k,l} > 0$ for some $1 \le l \le e_k$ and some $0 \le k \le n$. Let $\widetilde{\alpha}_{k,l-1} = \alpha_{k,l-1} + 1$, $\widetilde{\alpha}_{k,l} = \alpha_{k,l} - 1$, and set $\widetilde{\alpha}_{i,j} = \alpha_{i,j}$ otherwise, where $i \in \{0, \ldots, n\}$ and $j \in \{0, \ldots, e_i\}$. From the relations of Lemma 3.1 it follows that

$$\psi\left(X_{0,0}^{\widetilde{\alpha}_{0,0}}\cdots X_{0,e_0}^{\widetilde{\alpha}_{0,e_0}}\cdots X_{n,0}^{\widetilde{\alpha}_{n,0}}\cdots X_{n,e_n}^{\widetilde{\alpha}_{n,e_n}}\right)=Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0+1}Z_1^{\gamma_1-1},$$

which completes the proof. □

Corollary 3.3 *The set*

$$M:=\left\{Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}\in\mathbb{F}_q[\mathbf{Y},\mathbf{Z}]:\gamma_0+\gamma_1=\sum_{i=0}^{n}e_i\beta_i\right\},$$

is a basis for $\mathcal{B}$ as an $\mathbb{F}_q$-vector space.

From Corollary 2.3 we know that the cartesian product $\mathbb{P}^n(\mathbb{F}_q)\times\mathbb{P}^1(\mathbb{F}_q)$ and S have the same number of rational points, and the construction of S together with Proposition 2.2, suggest the bijection $\varphi\colon\mathbb{P}^n(\mathbb{F}_q)\times\mathbb{P}^1(\mathbb{F}_q)\to S$ defined by

$$\begin{aligned}&\varphi((a_0:\cdots:a_n),(b_0:b_1))\\&=\left(a_0b_0^{e_0}:a_0b_0^{e_0-1}b_1:\cdots:a_0b_1^{e_0}:\cdots:a_nb_0^{e_n}:a_nb_0^{e_n-1}b_1:\cdots:a_nb_1^{e_n}\right),\end{aligned}$$

where the points of $\mathbb{P}^n(\mathbb{F}_q)$ and $\mathbb{P}^1(\mathbb{F}_q)$ are always written in standard notation. For $i=1,\ldots,N$, let $Q_i=\varphi^{-1}(P_i)$, where $P_1,\ldots,P_N$ is the set of points of S used to define $C_S(d)$. Now define the $\mathbb{F}_q$-linear evaluation map

$$\begin{aligned}\widetilde{ev}_d:\mathcal{B}_d&\to\mathbb{F}_q^N\\f&\mapsto(f(Q_1),\ldots,f(Q_N)),\end{aligned}$$

where the evaluation of a monomial $Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}$ at such a pair is given as

$$Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}((a_0:\cdots:a_n),(b_0:b_1))=a_0^{\beta_0}\cdots a_n^{\beta_n}b_0^{\gamma_0}b_1^{\gamma_1}.$$

Lemma 3.4 *The diagram*

$$\begin{array}{ccc}\mathbb{F}_q[\mathbf{X}]_d & \xrightarrow{\ \psi\ } & \mathcal{B}_d\\ \Big\downarrow{\scriptstyle ev_d} & \swarrow{\scriptstyle \widetilde{ev}_d} & \\ \mathbb{F}_q^N & & \end{array}$$

is commutative and the image of $\widetilde{ev}_d$ is $C_S(d)$.

Proof Let $Q=((a_0:\cdots:a_n),(b_0:b_1))\in\mathbb{P}^n(\mathbb{F}_q)\times\mathbb{P}^1(\mathbb{F}_q)$ (with the points written in standard notation) and let $P=\varphi(Q)$ (also written in standard notation). Let $\mathbf{X}^{\boldsymbol{\alpha}}=X_{0,0}^{\alpha_{0,0}}\cdots X_{0,e_0}^{\alpha_{0,e_0}}\cdots X_{n,0}^{\alpha_{n,0}}\cdots X_{n,e_n}^{\alpha_{n,e_n}}\in\mathbb{F}_q[\mathbf{X}]_d$ be a monomial of degree d, then

$$\begin{aligned}\mathbf{X}^{\boldsymbol{\alpha}}(P)&=\left(a_0b_0^{e_0}\right)^{\alpha_{0,0}}\cdots\left(a_0b_1^{e_0}\right)^{\alpha_{0,e_0}}\cdots\left(a_nb_0^{e_n}\right)^{\alpha_{n,0}}\cdots\left(a_nb_1^{e_n}\right)^{\alpha_{n,e_n}}\\&=a_0^{\beta_0}\cdots a_n^{\beta_n}b_0^{\gamma_0}b_1^{\gamma_1},\end{aligned}$$

where $\beta_i=\sum_{j=0}^{e_i}\alpha_{i,j}$ for all $0\le i\le n$, $\sum_{i=0}^{n}\beta_i=d$, $\gamma_0=\sum_{i=0}^{n}\sum_{j=0}^{e_i}(e_i-j)\alpha_{i,j}$, and $\gamma_1=\sum_{i=0}^{n}\sum_{j=0}^{e_i}j\alpha_{i,j}$. Hence $Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}\in\mathcal{B}_d$ and

$$a_0^{\beta_0}\cdots a_n^{\beta_n}b_0^{\gamma_0}b_1^{\gamma_1}=Y_0^{\beta_0}\cdots Y_n^{\beta_n}Z_0^{\gamma_0}Z_1^{\gamma_1}(Q)=\psi(\mathbf{X}^{\boldsymbol{\alpha}})(Q).$$

This proves that the diagram is commutative and since ψ is surjective the images of ev_d and $\widetilde{ev}_d$ coincide. □

Let J_d be the kernel of $\widetilde{ev}_d$. As a consequence of the above result we have

$$\mathbb{F}_q[\mathbb{X}]_d/I_S(d) \simeq C_S(d) \simeq \mathcal{B}_d/J_d,$$

and $\psi^{-1}(J_d) = I_S(d)$. So an alternative construction of $C_S(d)$ is given, which will used to determine its dimension by finding a basis for $\mathcal{B}_d/J_d$. Clearly the classes in $\mathcal{B}_d/J_d$ of the monomials in the set M_d are a generating set for $\mathcal{B}_d/J_d$. Considering when two such monomials evaluate to the same value on the points $Q_1, \ldots, Q_N$, we are led to the following

Definition 3.5 Let $\widetilde{J}_d$ be the $\mathbb{F}_q$-vector subspace of $\mathcal{B}_d$ generated by the binomials of the type

$$Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} - Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1},$$

where $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$, $Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1} \in M_d$, and for all $i \in \{0, \ldots, n\}$ we have

$$\begin{aligned} &\beta_i \equiv \tilde{\beta}_i \pmod{q-1}, \quad \gamma_i \equiv \tilde{\gamma}_i \pmod{q-1}, \\ &\beta_i = 0 \iff \tilde{\beta}_i = 0, \quad \gamma_i = 0 \iff \tilde{\gamma}_i = 0. \end{aligned}$$

Clearly $\widetilde{J}_d \subset J_d$, and it will be shown that equality holds. We define a total order in the set M_d by stating that

$$Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \prec Y_0^{\overline{\beta}_0} \cdots Y_n^{\overline{\beta}_n} Z_0^{\overline{\gamma}_0} Z_1^{\overline{\gamma}_1},$$

if the first nonzero entry from left to right in $(\beta_0 - \overline{\beta}_0, \ldots, \beta_n - \overline{\beta}_n, \gamma_0 - \overline{\gamma}_0)$ is negative.

In what follows we will denote the class of a monomial $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ in the quotient space $\mathcal{B}_d/\widetilde{J}_d$ by $[Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}]$.

Lemma 3.6 *Let $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \mathcal{B}_d$, let $j := max\{0 \le i < n : \beta_i \neq 0\}$. Then the least monomial in the class $[Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}]$ is $Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1}$ where*

$$\tilde{\beta}_i = \begin{cases} 0 & \text{if } \beta_i = 0, i \in \{0, \ldots, n\}, \\ a \text{ with } 1 \le a \le q-1,\ a \equiv \beta_i \pmod{q-1} & \text{if } 0 \le i < j \text{ and } \beta_i \neq 0, \\ d - \sum_{s=0}^{j-1} \tilde{\beta}_s & \text{if } i = j, \end{cases}$$

$$\tilde{\gamma}_0 = \begin{cases} 0 & \text{if } \gamma_0 = 0, \\ b \text{ with } 1 \le b \le q-1, b \equiv \gamma_0 \pmod{q-1} & \text{if } 0 < \gamma_0 < \sum_{i=0}^{j} \beta_i e_i, \\ \sum_{i=0}^{j} \tilde{\beta}_i e_i & \text{if } \gamma_0 = \sum_{i=0}^{j} \beta_i e_i, \end{cases}$$

and $\tilde{\gamma}_1 := \sum_{i=0}^{j} \tilde{\beta}_i e_i - \tilde{\gamma}_0$.

Proof From the definition of $\tilde{\beta}_0, \ldots, \tilde{\beta}_n$, $\tilde{\gamma}_0$ and $\tilde{\gamma}_1$, it follows that the monomial $Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1}$ is in $\mathcal{B}_d$ and that

$$Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1} - Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1} \in \widetilde{J}_d.$$

Also from the definitions above, it is clear that, for $j+1 \leq i \leq n$ we have $\tilde{\beta}_i = 0$, because $\beta_i = 0$ for $i \geq j+1$. Moreover, for $0 \leq i \leq j-1$, the value of $\tilde{\beta}_i$ is the least possible. Thus, if $Y_0^{\delta_0} \cdots Y_n^{\delta_n} Z_0^{\theta_0} Z_1^{\theta_1} \in [Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}]$ and $\delta_i > \tilde{\beta}_i$ for some $i \in \{0, \ldots, j-1\}$, we have

$$Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1} \prec Y_0^{\delta_0} \cdots Y_n^{\delta_n} Z_0^{\theta_0} Z_1^{\theta_1}.$$

If $\delta_i = \tilde{\beta}_i$ for $i \in \{0, \ldots, j-1\}$, by observing that $\delta_i = 0$ for $i \in \{j+1, \ldots, n\}$, $\delta_j = d - \sum_{s=0}^{j-1} \tilde{\beta}_s = \tilde{\beta}_j$. Since $\tilde{\gamma}_0$ also has the least possible value we must have

$$Y_0^{\tilde{\beta}_0} \cdots Y_n^{\tilde{\beta}_n} Z_0^{\tilde{\gamma}_0} Z_1^{\tilde{\gamma}_1} \preceq Y_0^{\delta_0} \cdots Y_n^{\delta_n} Z_0^{\theta_0} Z_1^{\theta_1},$$

completing the proof. □

We now collect the monomials which are minimal in their classes.

Definition 3.7 Let $\Delta(\mathcal{B})_d$ be the set of monomials $Y_0^{\beta_0} \cdots Y_j^{\beta_j} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \mathcal{B}_d$ such that $Y_0^{\beta_0} \cdots Y_j^{\beta_j} Z_0^{\gamma_0} Z_1^{\gamma_1}$ is the minimal element of $[Y_0^{\beta_0} \cdots Y_j^{\beta_j} Z_0^{\gamma_0} Z_1^{\gamma_1}]$.

Observe that given a polynomial $g \in \mathcal{B}_d$ there exists a polynomial $\widetilde{g}$ in the $\mathbb{F}_q$-space $\langle \Delta(\mathcal{B})_d \rangle$ generated by $\Delta(\mathcal{B})_d$ such that $g - \widetilde{g} \in \widetilde{J}_d$.

Proposition 3.8 *Let h be an $\mathbb{F}_q$-linear combination of elements of $\Delta(\mathcal{B})_d$ such that $h(Q) = 0$ for all $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. Then $h = 0$.*

Proof From [15] we know that the vanishing ideal of $\mathbb{P}^n(\mathbb{F}_q)$ is

$$I_n = \langle Y_i^q Y_j - Y_i Y_j^q \ : \ 0 \leq i < j \leq n \rangle \subset \mathbb{F}_q[Y_0, \ldots, Y_n],$$

and moreover, that the set of the given generators of this ideal is a Gröbner basis for I_n with respect to the lexicographic order where $Y_0 > \cdots > Y_n$. From a well-known result from Gröbner bases ([1, Prop. 6.52]) it follows that the classes in $\mathbb{F}_q[Y_0, \ldots, Y_n]/I_n$ of the set $\Delta(I_n)$, consisting of all monomials of the form $Y_0^{\beta_0} \cdots Y_j^{\beta_j}$, where $j \in \{0, \ldots, n\}$, $\beta_j \neq 0$, $\beta_i = 0$ if $i > j$, and $0 \leq \beta_i \leq q-1$ if $0 \leq i < j$, is a basis for $\mathbb{F}_q[Y_0, \ldots, Y_n]/I_n$ as an $\mathbb{F}_q$-vector space. The set $\Delta(I_n)$ is formed by all monomials which are not multiples of any of the leading monomials of the generators of I_n, and it is easy to verify that

$$\Delta(I_n)_d = \left\{ Y_0^{\beta_0} \cdots Y_n^{\beta_n} \in \Delta(I_n) \ : \ \deg(Y_0^{\beta_0} \cdots Y_n^{\beta_n}) = d \right\},$$

is a basis for the quotient $\mathbb{F}_q[Y_0, \ldots, Y_n]_d / I_n(d)$, where in $\mathbb{F}_q[Y_0, \ldots, Y_n]_d$ and $I_n(d)$ there are only homogeneous polynomials of degree d.

Let us write $I_1 = \langle Z_0^q Z_1 - Z_0 Z_1^q \rangle \subset F_q[Z_0, Z_1]$, so that

$$\Delta(I_1)_d = \left\{ Z_0^{\gamma_0} Z_1^{\gamma_1} \ : \ \gamma_0 + \gamma_1 = d \text{ and either } \gamma_1 = 0 \text{ or } 0 \leq \gamma_0 \leq q-1 \right\},$$

and let $\rho(\beta_1, \ldots, \beta_n) = \sum_{i=0}^n e_i \beta_i$. Then from Lemma 3.6 it follows that the elements of $\Delta(\mathcal{B})_d$ are exactly the monomials of the form $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ with $Y_0^{\beta_0} \cdots Y_n^{\beta_n} \in \Delta(I_n)_d$ and $Z_0^{\gamma_0} Z_1^{\gamma_1} \in \Delta(I_1)_{\rho(\beta_1, \ldots, \beta_n)}$.

We abbreviate the sequences $(\beta_0, \ldots, \beta_n)$ and (γ_0, γ_1) by $\boldsymbol{\beta}$ and $\boldsymbol{\gamma}$ respectively, and also write $\mathbf{Y}^{\boldsymbol{\beta}}$ for $Y_0^{\beta_0} \cdots Y_n^{\beta_n}$ and $\mathbf{Z}^{\boldsymbol{\gamma}}$ for $Z_0^{\gamma_0} Z_1^{\gamma_1}$. Let

$$h = \sum_{\mathbf{Y}^{\boldsymbol{\beta}} \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(\mathcal{B})_d} c_{(\boldsymbol{\beta}; \boldsymbol{\gamma})} \mathbf{Y}^{\boldsymbol{\beta}} \mathbf{Z}^{\boldsymbol{\gamma}},$$

be an $\mathbb{F}_q$-linear combination of elements of $\Delta(\mathcal{B})_d$ such that $h(Q) = 0$ for all $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$, and let $(b_0 : b_1) \in \mathbb{P}^1(\mathbb{F}_q)$. Then

$$h_{(b_0:b_1)} := \sum_{\mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d} \left(\sum_{\substack{\boldsymbol{\gamma} \text{ such that} \\ \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{\rho(\boldsymbol{\beta})}}} c_{(\boldsymbol{\beta};\boldsymbol{\gamma})} b_0^{\gamma_0} b_1^{\gamma_1} \right) \mathbf{Y}^{\boldsymbol{\beta}},$$

vanishes at all points of $\mathbb{P}^n(\mathbb{F}_q)$, hence it is an element of $I_n(d)$. As $\Delta(I_n)_d$ is a basis for the quotient $\mathbb{F}_q[Y_0, \ldots, Y_n]_d / I_n(d)$,

$$\sum_{\substack{\boldsymbol{\gamma} \text{ such that} \\ \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{\rho(\boldsymbol{\beta})}}} c_{(\boldsymbol{\beta};\boldsymbol{\gamma})} Z_0^{\gamma_0} Z_1^{\gamma_1}$$

vanishes at all points of $\mathbb{P}^1(\mathbb{F}_q)$, for all $\boldsymbol{\beta}$ such that $\mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d$. Similarly, since $\Delta(I_1)_{\rho(\boldsymbol{\beta})}$ is a basis for the quotient $\mathbb{F}_q[Z_0, Z_1]_d / I_1(d)$, $c_{(\boldsymbol{\beta};\boldsymbol{\gamma})} = 0$ whenever $\mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(I_1)_{\rho(\boldsymbol{\beta})}$ and $\mathbf{Y}^{\boldsymbol{\beta}} \in \Delta(I_n)_d$, or equivalently, whenever $\mathbf{Y}^{\boldsymbol{\beta}} \mathbf{Z}^{\boldsymbol{\gamma}} \in \Delta(\mathcal{B})_d$. □

There are two important consequences of the above result.

Proposition 3.9 $J_d = \widetilde{J}_d$.

Proof Clearly, $\widetilde{J}_d \subset J_d$. Let $g \in J_d$ and let $\widetilde{g} \in \langle \Delta(\mathcal{B})_d \rangle$ be such that $g - \widetilde{g} \in \widetilde{J}_d$. Then $g(Q) = \widetilde{g}(Q)$ for all $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$, so $\widetilde{g}(Q) = 0$ for all $Q \in \mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$. From the above result it follows that $\widetilde{g} = 0$ and hence $g \in \widetilde{J}_d$. □

Proposition 3.10 *The classes in B_d/J_d of the monomials in $\Delta(\mathcal{B})_d$ form a basis for B_d/J_d as an $\mathbb{F}_q$-vector space.*

Proof Clearly the classes of the monomials of $\Delta(\mathcal{B})_d$ generate B_d/J_d as an $\mathbb{F}_q$-vector space, and from Proposition 3.8 it follows that the set of these classes is linearly independent. □

4 On the dimension of $C_S(d)$

From Proposition 3.10 it follows that that $\dim C_S(d) = |\Delta(\mathcal{B})_d|$, and in this section we present some formulas to determine $|\Delta(\mathcal{B})_d|$. Recall that the elements of $\Delta(\mathcal{B})_d$ are exactly the monomials of the form $Y_0^{\beta_0} \cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1}$ where for $j \in \{0, \ldots, n\}$, $\beta_j \neq 0$, $\beta_i = 0$ if $i > j$; $0 \leq \beta_i \leq q-1$ if $0 \leq i < j$ and $\sum_{i=0}^{j} \beta_i = d$, and also $\gamma_0 + \gamma_1 = \sum_{i=0}^{j} e_i \beta_i$ with either $\gamma_1 = 0$ or $0 \leq \gamma_0 \leq q-1$. For a fixed $j \in \{0, \ldots, n\}$, the maximal value for $\gamma_0 + \gamma_1$ is $e_0(d-1) + e_j$, which is the value of $\sum_{i=0}^{j} e_i \beta_i$ when $\beta_0 = d$, in the case $j = 0$, or $\beta_0 = d-1$, $\beta_j = 1$ and $\beta_i = 0$ if $0 < i < j$, in the case $1 \leq j \leq n$. Indeed if $\tilde{\beta}_0, \ldots, \tilde{\beta}_j$ are such that $\sum_{i=0}^{j} \tilde{\beta}_i = d$, $\tilde{\beta}_j \neq 0$, and $\tilde{\beta}_k \neq 0$ for some $0 < k < j$, then $\tilde{\beta}_0 < d-1$ and

$$e_0(\tilde{\beta}_0 + 1) + e_k(\tilde{\beta}_k - 1) + \sum_{i=1, i \neq k}^{j} e_i \tilde{\beta}_i - \sum_{i=0}^{j} e_i \tilde{\beta}_i = e_0 - e_k \geq 0$$

which shows that the maximal value of $\sum_{i=0}^{j} e_i\beta_i$ is assumed when $\beta_k = 0$ for $0 < k < j$. Similarly, it can be shown that we can assume $\beta_j = 1$. We write $\sum_{i=0}^{j} e_i\beta_i$ as

$$\sum_{i=0}^{j} e_i\beta_i = \sum_{i=0}^{j-1} e_i\beta_i + e_j\left(d - \sum_{i=0}^{j-1}\beta_i\right) = \sum_{i=0}^{j-1} m_{i,j}\beta_i + e_j d,$$

where $m_{i,j} := e_i - e_j$ for $0 \le i < j \le n$, and accordingly write $e_0(d-1) + e_j = (e_0 - e_j)(d-1) + e_j d = m_{0,j}(d-1) + e_j d$.

For $j \in \{1, \ldots, n\}$, let $\mathcal{A}_d(j, s)$ be the number of integer solutions of the system

$$\begin{cases} \beta_0 + \cdots + \beta_{j-1} + \beta_j & = d \\ m_{0,j}\beta_0 + \cdots + m_{j-1,j}\beta_{j-1} & = s \end{cases} \tag{1}$$

where $0 \le s \le m_{0,j}(d-1)$ with the restrictions $\beta_j > 0$ and $0 \le \beta_i < q$ for $0 \le i < j$, and for $j \in \{0, \ldots, n\}$ let,

$$\Delta(\mathcal{B})_{d,j} = \{Y_0^{\beta_0} \cdots Y_j^{\beta_j} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \Delta(\mathcal{B})_d \mid \beta_j > 0 \text{ and } \beta_i = 0 \text{ for } j < i \le n\}.$$

Observe that $|\Delta(\mathcal{B})_d| = \sum_{j=0}^{n} \left|\Delta(\mathcal{B})_{d,j}\right|$. From Lemma 3.6 it is easy to see that $|\Delta(\mathcal{B})_{d,0}| = \min(q-1, e_0 d - 1) + 2$. In the following proposition a formula for $|\Delta(\mathcal{B})_{d,j}|$ when $1 \le j \le n$ is presented.

Proposition 4.1 *For $j \in \{1, \ldots, n\}$,*

$$|\Delta(\mathcal{B})_{d,j}| = \sum_{s=0}^{q-e_j d} (e_j d + s + 1)\mathcal{A}_d(j, s) + (q+1) \sum_{s=q-e_j d+1}^{m_{0,j}(d-1)} \mathcal{A}_d(j, s).$$

Proof If $\beta_0, \ldots, \beta_j$ are nonnegative integers such that $\sum_{i=0}^{j} \beta_j = d$, $\beta_j > 0$ and $0 \le \beta_i < q$ for $0 \le i < j$, then $Y_0^{\beta_0} \cdots Y_j^{\beta_j} Z_0^{\gamma_0} Z_1^{\gamma_1} \in \Delta(\mathcal{B})_{d,j}$ for all $\gamma_0 \in \{0, \ldots, \min(q - 1, \sum_{i=0}^{j} e_i\beta_i - 1)\} \cup \{\sum_{i=0}^{j} e_i\beta_i\}$ (with $\gamma_1 = \sum_{i=0}^{j} e_i\beta_i - \gamma_0$).

As above, we write $\sum_{i=0}^{j} e_i\beta_i = s + e_j d$, where $s = \sum_{i=0}^{j-1} m_{i,j}\beta_i$. If $\sum_{i=0}^{j} e_i\beta_i > q$, (equivalently, if $s > q - e_j d$), then there are exactly $q+1$ different choices for γ_0, namely $\{0, \ldots, q-1, s + e_j d\}$. If $\sum_{i=0}^{j} e_i\beta_i \le q$, (equivalently, if $s \le q - e_j d$), then there are $\sum_{i=0}^{j} e_i\beta_i + 1$ different choices for γ_0, namely $\{0, \ldots, s + e_j d\}$. □

The next result presents a method to determine $\mathcal{A}_d(j, s)$.

Lemma 4.2 *For $j \in \{1, \ldots, n\}$ and $s \in \{0, \ldots, m_{0,j}(d-1)\}$,*

$$\mathcal{A}_d(j, s) = \frac{1}{d!s!} \frac{\partial^{d+s} g}{\partial^d x\, \partial^s y}(0, 0),$$

where

$$g(x, y) = \frac{x}{1-x} \cdot \prod_{i=0}^{j-1} \frac{1 - x^q y^{q m_{i,j}}}{1 - x y^{m_{i,j}}}.$$

Proof We use ideas from generating function theory to find the number of solutions of the system (1) above. For basic results on generating functions, we refer for example to Chapter six of [19]. Let $j \in \{1, \ldots, n\}$ and consider the series $g(x, y)$ defined as

$$\begin{aligned} g(x, y) &= (x + x^2 + \cdots) \prod_{i=0}^{j-1} \left(1 + xy^{m_{i,j}} + \cdots + (xy^{m_{i,j}})^{q-1}\right) \\ &= \frac{x}{1-x} \cdot \prod_{i=0}^{j-1} \frac{1 - x^q y^{qm_{i,j}}}{1 - xy^{m_{i,j}}}. \end{aligned}$$

For $0 \leq i < j$ the exponents of x and y in the term $1 + xy^{m_{i,j}} + \cdots + (xy^{m_{i,j}})^{q-1}$ can be thought of as representing the possible choices for the values of β_i and $m_{i,j}\beta_i$, respectively, which appear in the second equation of the system (1) for a fixed $s \in \{0, \ldots, m_{0,j}(d-1)\}$. Similarly, the exponents of x in the term $(x + x^2 + \cdots)$ can be though as representing the possible choices for the value of β_j, which appear in the first equation of system (1). Hence, the coefficient of $x^d y^s$ in this expression yields the number of solutions of (1) and can be given as

$$\frac{1}{d!s!} \frac{\partial^{d+s} g}{\partial^d x \, \partial^s y}(0, 0).$$

□

Now the dimension of $C_S(d)$ is determined in some cases.

Proposition 4.3 *If* $d > \dfrac{q-1}{e_n}$, *then*

$$\dim(C_S(d)) = (q+1) \sum_{j=0}^{n} \sum_{i=0}^{j} (-1)^i \binom{j}{i} \binom{j + d - 1 - iq}{d - 1 - iq}.$$

Proof From Proposition 4.1 it follows that $\dim(C_S(d)) = |\Delta(\mathcal{B})_d| = \min(q-1, e_0 d - 1) + 2 + \sum_{j=1}^{n} |\Delta(\mathcal{B})_{d,j}|$. For all $j \in \{0, \ldots, n\}$, $e_j d \geq e_n d > q - 1$, and in particular $\min(q-1, e_0 d - 1) + 2 = q + 1$. When $1 \leq j \leq n$, $q - e_j d < 1$ and if $q - e_j d = 0$, for $s = 0$ we have $e_j d + s + 1 = q + 1$, so from Proposition 4.1 it follows that

$$|\Delta(\mathcal{B})_{d,j}| = (q+1) \sum_{s=0}^{m_{0,j}(d-1)} \mathcal{A}_d(j, s).$$

Observe that $\sum_{s=0}^{m_{0,j}(d-1)} \mathcal{A}_d(j, s)$ counts the number of integer solutions of the equation $\beta_0 + \cdots + \beta_j = d$ with the restrictions $\beta_j > 0$ and $0 \leq \beta_i < q$ for $0 \leq i < j$. This is equivalent to determining the coefficient of x^d in the expression

$$\begin{aligned} &(1 + x + x^2 + \cdots + x^{q-1})^j (x + x^2 + \cdots) \\ &= x \left(\frac{1 - x^q}{1 - x}\right)^j \left(\frac{1}{1 - x}\right) \\ &= x(1 - x^q)^j \left(\frac{1}{1 - x}\right)^{j+1} \\ &= x \left[\sum_{i=0}^{j} (-1)^i \binom{j}{i} x^{iq}\right] \left[\sum_{k=0}^{\infty} \binom{k + j}{k} x^k\right] \end{aligned}$$

which is given by

$$\sum_{i=0}^{j}(-1)^i\binom{j}{i}\binom{j+d-1-iq}{d-1-iq}.$$

Since this summation is equal to 1 when $j=0$, the result is obtained by summing up these expressions from $j=0$ to $j=n$ and multiplying the result by $q+1$. □

Proposition 4.4 *If $d > n(q-1)$, then*

$$\dim(C_S(d)) = (q+1)(q^n+q^{n-1}+\cdots+1).$$

Proof For $d > n(q-1)$, $d \geq n(q-1)+1 \geq (q-1)+1 = q$. Since $d \leq e_n d$, $e_n d > q-1$, a similar argument as in the previous proposition gives

$$\dim(C_S(d)) = (q+1) + \sum_{j=1}^{n}(q+1)\sum_{s=0}^{m_{0,j}(d-1)}\mathcal{A}_d(j,s).$$

Since $d > q$, the number of integer solutions of the equation $\beta_0+\cdots+\beta_j = d$ with the restrictions $\beta_j > 0$ and $0 \leq \beta_i < q$ for $0 \leq i < j$ is q^j, therefore

$$\sum_{s=0}^{m_{0,j}(d-1)}\mathcal{A}_d(j,s) = q^j.$$

□

We end this section by giving some numerical examples of the parameters of projective Reed–Muller type codes over a scroll. These examples were obtained by using the computational software Magma [4]. They illustrate the case when $e_i \neq e_j$ when $i \neq j$, for $i, j \in \{0,\ldots,n\}$. In the next section we will determine the parameters of $C_s(d)$ for all relevant values of d in the case when $e_0 = \cdots = e_n$.

Example 4.5 Consider the scroll $S := S_{3,2,1}$ defined over the field with 4 elements $\mathbb{F}_4$. The following table shows the basic parameters of the code $C_S(d)$ as d varies from 1 to 7.

d	Length	Dimension	Minimum distance
1	105	9	32
2	105	27	12
3	105	49	8
4	105	75	4
5	105	90	3
6	105	100	2
7	105	105	1

5 The parameters of $C_S(d)$ in a special case

Let θ be the isomorphism between the $\mathbb{F}_q$-vector space $M_{N_1\times N_2}(\mathbb{F}_q)$ of $N_1 \times N_2$ matrices and $\mathbb{F}_q^{N_1N2}$, given by

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1N_2} \\ a_{21} & a_{22} & \cdots & a_{2N_2} \\ \vdots & \vdots & \cdots & \vdots \\ a_{N_11} & a_{22} & \cdots & a_{N_1N_2} \end{pmatrix} \mapsto \left(a_{11}, a_{12}, \ldots, a_{1N_2}, \ldots, a_{N_11}, a_{N_12}, \ldots, a_{N_1N_2}\right)$$

We recall the concept of direct product of codes, as presented in [20, p. 36], slightly modified for our purposes.

Definition 5.1 Let $C_i \subseteq \mathbb{F}_q^{n_i}$ be a linear code, where n_i is a nonnegative integer for $i = 1, 2$, and let $M_{n_1\times n_2}(\mathbb{F}_q)$ be the linear space of $n_1 \times n_2$ matrices with entries in $\mathbb{F}_q$. The direct product of C_1 and C_2, denoted by $C_1 \underline{\otimes} C_2$, is defined as the image, under θ, of all matrices in $M_{n_1\times n_2}(\mathbb{F}_q)$ the rows of which belong to C_2 and the columns of which belong to C_1.

Proposition 5.2 *Let $C_i \subseteq \mathbb{F}_q^{n_i}$ be a linear code which has dimension k_i and minimum distance δ_i for $i = 1, 2$. Then,*

1. *$C_1 \underline{\otimes} C_2$ has length n_1n_2, dimension k_1k_2 and minimum distance $\delta_1\delta_2$.*
2. *If $\{u_i : 1 \le i \le k_1\}$ is a basis for C_1 and $\{v_j : 1 \le j \le k_2\}$ is a basis for C_2, then $\{\theta(u_i^T v_j) : 1 \le i \le k_1, 1 \le j \le k_2\}$ is a basis for $C_1 \underline{\otimes} C_2$, where u_i^T is an $n_1 \times 1$ matrix and v_j is a $1 \times n_2$ matrix.*

Proof The first part is proved in [20], Theorems 2.5.2 and 2.5.3. The second part is a consequence of Lemma 2.3 in [18]. □

These results will be used to determine the true minimum distance of $C_S(d)$ in a special case (cf. [5, Thm. 5.8]). Before doing so, we briefly recall the basic data on projective Reed–Muller codes. Let d and m be positive integers and let $N_m = q^m + \cdots + q + 1$. Denoting the points of $\mathbb{P}^m(\mathbb{F}_q)$ by $U_1, \ldots, U_{N_m}$, we recall that the projective Reed–Muller code (of order d, over $\mathbb{P}^m(\mathbb{F}_q)$) is the image $\mathrm{PRM}(d, m)$ of the evaluation morphism

$$\begin{array}{rcl} \varphi_{d,m} : \mathbb{F}_q[Y_0, \ldots, Y_m]_d & \to & \mathbb{F}_q^{N_m} \\ f & \mapsto & \left(f(U_1), \ldots, f\left(U_{N_m}\right)\right), \end{array}$$

defined over the space of homogeneous polynomials of degree d, and where, for evaluation purposes, the points of $\mathbb{P}^m(\mathbb{F}_q)$ are written in standard notation. From [17] (see also [15]) we know that if $d \ge m(q-1)$ then $\varphi_{d,m}$ is surjective, and that for $1 \le d \le m(q-1)$ the dimension and minimum distance $\delta_{\mathrm{PRM}}(d, m)$ of $\mathrm{PRM}(d, m)$ are as follows:

$$\dim(\mathrm{PRM}(d, m)) = \sum_{j=0}^{m}\sum_{i=0}^{j}(-1)^i \binom{j}{i}\binom{j+d-1-iq}{d-1-iq},$$

$$\delta_{\mathrm{PRM}}(d, m) = (q-r)q^{m-k-1},$$

where $d - 1 = k(q-1) + r$ and $0 \le r < q-1$. In the formula for the dimension we assume $\binom{a}{b} = 0$ if $b < 0$, so for example, if $d \le q$ then

$$\dim(\mathrm{PRM}(d, m)) = \sum_{j=0}^{m}\binom{j+d-1}{d-1} = \binom{d+m}{d},$$

a formula first established by Lachaud (see [14]).

Let $d_1 = \dim(\mathrm{PRM}(d,m))$. From [17] we also know that there are monomials $\mathbf{Y}^{\boldsymbol{\beta}_1},\ldots,\mathbf{Y}^{\boldsymbol{\beta}_{d_1}}$ in $\mathbb{F}_q[Y_0,\ldots,Y_m]_d$ such that $\{\varphi_{d,m}(\mathbf{Y}^{\boldsymbol{\beta}_1}),\ldots,\varphi_{d,m}(\mathbf{Y}^{\boldsymbol{\beta}_{d_1}})\}$ is a basis for $\mathrm{PRM}(d,m)$.

Proposition 5.3 *Assume $e_0 = e_1 = \cdots = e_n = e$. Then,*

$$C_S(d) \cong \mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1).$$

Proof Let $N = (q+1)(q^n+\cdots+q+1)$. We know from Lemma 3.4 that $C_S(d) = \widetilde{ev}_d(\mathcal{B}_d) \subset \mathbb{F}_q^N$, so $C_S(d)$ is generated by the vectors $\widetilde{ev}_d(Y_0^{\beta_0}\cdots Y_n^{\beta_n} Z_0^{\gamma_0} Z_1^{\gamma_1})$ where $\sum_{i=0}^n \beta_i = d$ and, since $e_0 = e_1 = \cdots = e_n = e$, $\gamma_0+\gamma_1 = de$. As mentioned above, from [17] we know that, setting $d_1 = \dim(\mathrm{PRM}(d,n))$, there are monomials $\mathbf{Y}^{\boldsymbol{\beta}_1},\ldots,\mathbf{Y}^{\boldsymbol{\beta}_{d_1}}$ in $\mathbb{F}_q[Y_0,\ldots,Y_n]_d$ and elements $h_1,\ldots,h_{d_1} \in \mathbb{F}_q$ such that

$$Y_0^{\beta_0}\cdots Y_n^{\beta_n}(a_0,\ldots,a_n) = \sum_{i=1}^{d_1} h_i \mathbf{Y}^{\boldsymbol{\beta}_i}(a_0,\ldots,a_n),$$

for all $(a_0:\cdots:a_n) \in \mathbb{P}^n(\mathbb{F}_q)$. In the same way, setting $d_2 = \dim(\mathrm{PRM}(de,1))$ monomials $\mathbf{Z}^{\boldsymbol{\gamma}_1},\ldots,\mathbf{Z}^{\boldsymbol{\gamma}_{d_2}}$ exists in $\mathbb{F}_q[Z_0,Z_1]_{de}$, and elements $g_1,\ldots,g_{d_2} \in \mathbb{F}_q$ such that

$$Z_0^{\gamma_0} Z_1^{\gamma_1}(b_0,b_1) = \sum_{j=1}^{d_2} g_j \mathbf{Z}^{\gamma_j}(b_0,b_1),$$

so $C_S(d)$ is generated by the vectors $\widetilde{ev}_d(\mathbf{Y}^{\boldsymbol{\beta}_i}\mathbf{Z}^{\gamma_j})$ where $i = 1,\ldots,d_1$ and $j = 1,\ldots,d_2$.

On the other hand, from Proposition 5.2 and the data on projective Reed–Muller codes, $\mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1) \subset \mathbb{P}^{N_n N_1}(\mathbb{F}_q)$, where $N_n = q^n+\cdots+q+1$, $N_1 = q+1$, and

$$\{\theta(\varphi_{d,n}(\mathbf{Y}^{\boldsymbol{\beta}_i})^{\mathsf{T}}\varphi_{de,1}(\mathbf{Z}^{\boldsymbol{\gamma}_j})) \,:\, i = 1,\ldots,d_1;\ j = 1,\ldots,d_2\},$$

is a basis for $\mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1)$.

For $i \in \{1,\ldots,d_1\}$ and $j \in \{1,\ldots,d_2\}$ the entries in either vector $\widetilde{ev}_d(\mathbf{Y}^{\boldsymbol{\beta}_i}\mathbf{Z}^{\gamma_j})$ or $\theta(\varphi_{d,n}(\mathbf{Y}^{\boldsymbol{\beta}_i})^{\mathsf{T}}\varphi_{de,1}(\mathbf{Z}^{\boldsymbol{\gamma}_j}))$ are of the same form, namely

$$a_0^{\beta_0}\cdots a_n^{\beta_n} b_0^{\gamma_0} b_1^{\gamma_1},$$

each entry carrying the data of one of the $(q^n+\cdots+q+1)(q+1)$ rational points of the cartesian product $\mathbb{P}^n(\mathbb{F}_q) \times \mathbb{P}^1(\mathbb{F}_q)$, the only difference between the vectors being (possibly) on the order under which the points appear. This proves that $C_S(d) \cong \mathrm{PRM}(d,n) \underline{\otimes} \mathrm{PRM}(de,1)$. □

We denote by $\delta(C_S(d))$ the minimum distance of $C_S(d)$.

Corollary 5.4 *Assume that $e_0 = e_1 = \cdots = e_n = e$, then the dimension and the minimum distance of $C_S(d)$ are as follows:*

If $d \geq n(q-1)$ then,

$$\dim(C_S(d)) = (q^n+\cdots+q+1)(q+1) \ \text{ and } \ \delta(C_S(d)) = 1.$$

If $(q-1)/e < d \leq n(q-1)$ then,

$$\dim(C_S(d)) = (q+1)\sum_{j=0}^{n}\sum_{i=0}^{j}(-1)^i \binom{j}{i}\binom{j+d-1-iq}{d-1-iq} \ \text{ and}$$

$$\delta(C_S(d)) = (q-r)q^{n-k-1}, \ \text{where } d-1 = k(q-1)+r \text{ and } 0 \leq r < q-1.$$

If $1 \leq d \leq (q-1)/e$ *then,*

$$\dim(C_S(d)) = (de+1)\binom{n+d}{d} \text{ and}$$
$$\delta(C_S(d)) = (q-d+1)(q-de+1)q^{n-1}.$$

Proof This is a consequence of the two Propositions above and the data on the projective Reed–Muller codes. We note that if $d \geq n(q-1)$ then $de \geq (q-1)$ so $\mathrm{PRM}(d,n) = \mathbb{F}_q^{q^n+\cdots+q+1}$ and $\mathrm{PRM}(de,1) = \mathbb{F}_q^{q+1}$. If $(q-1)/e < d \leq n(q-1)$, $de > q-1$ so $\mathrm{PRM}(de,1) = \mathbb{F}_q^{q+1}$. And if $1 \leq d \leq (q-1)/e$, then $de < q-1$ and a fortiori $d < q-1$, so Lachaud's formula can be applied for the dimension of $\mathrm{PRM}(d,n)$ and $\mathrm{PRM}(de,1)$. □

Acknowledgements The second author is grateful to Prof. F. Zaldivar for pointing out the concept of a higher dimensional scroll. We thank the referees for a careful reading and their comments which improved the manuscript.

References

1. Becker T., Weispfenning W.: Gröbner Bases. Springer, New York (1993).
2. Beelen, P., Datta, M., Ghorpade, S.R.: A combinatorial approach to the number of solutions of systems of homogeneous polynomial equations over finite fields. arXiv:1807.01683v2 (2018)
3. Beelen P., Datta M., Ghorpade S.R.: Maximum number of common zeros of homogeneous polynomials over finite fields. Proc. Am. Math. Soc. **146**(4), 1451–1468 (2018).
4. Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997).
5. Carvalho C., Neumann V.G.L.: Projective Reed-Muller type codes on rational normal scrolls. Finite Fields Appl. **37**, 85–107 (2016).
6. Carvalho C., Neumann V.G.L., Lopez H.: Projective nested cartesian codes. Bull. Braz. Math. Soc. **48**, 283–302 (2017).
7. Couvreur A., Duursma I.: Evaluation codes from smooth quadric surfaces and twisted Segre varieties. Des. Codes Cryptogr. **66**, 291–303 (2013).
8. Cox D., Little J., O'Shea D.: Ideals, Varieties, and Algorithms, 3rd edn. Springer, New York (2007).
9. Duursma I., Rentería C., Tapia-Recillas H.: Reed Muller codes on complete intersections. Appl. Algebra Eng. Commun. Comput. (AAECC) **11**, 455–462 (2001).
10. González-Sarabia, M., Martínez-Bernal, J., Villarreal, R.H., Vívares, C.E.: Generalized minimum distance functions. J. Algebr. Comb. https://doi.org/10.1007/s10801-018-0855-x (2018)
11. González-Sarabia M., Rentería C., Tapia Recillas H.: Reed-Muller type codes over the segre variety. Finite Fields Appl. **8**, 511–518 (2002).
12. González-Sarabia M., Rentería C.: The dual code of some Reed-Muller-type codes. Appl. Algebra Eng. Commun. Comput. (AAECC) **14**, 329–333 (2004).
13. Harris, J.: Algebraic Geometry: A First Course, 3rd. edn, Springer, GTM, no. 133 (1995)
14. Lachaud G.: Projective Reed-Muller codes. In: Cohen G., Godlewski P. (eds.) Coding Theory and Applications. Lecture Notes in Computer Science, vol. 311. Springer, Berlin (1988).
15. Rentería C., Tapia-Recillas H.: Reed-Muller codes: an ideal theory approach. Commun. Algebra **25**(2), 401–413 (1997).
16. Rentería, C., Tapia-Recillas, H.: Reed-Muller type codes on the Veronese Variety over finite fields. In: Buchmann, J., Hoholdt, T., Stichtenoth, H., Tapia-Recillas, H. (eds.) Coding Theory, Cryptography and Related Areas, ISBN 3-540-66248-0, pp. 237–243 , Springer, New York (2000)
17. Sörensen A.B.: Projective Reed-Muller codes. IEEE Trans. Inform. Theory **37**(6), 1567–1576 (1991).
18. Tochimani A., Pinto M.V., Villarreal R.H.: Direct products in projective Segre codes. Finite Fields Appl. **39**, 96–110 (2016).
19. Tucker A.: Applied Combinatorics, 6th edn. Wiley, New York (2012).
20. van Lint, J.H.: Coding Theory, Lect. Notes Math., 2nd edn, vol. 201. Springer, Berlin (1973)