HAL open science

Evaluation codes from smooth quadric surfaces and twisted Segre varieties

Alain Couvreur, Iwan Duursma

To cite this version:

Alain Couvreur, Iwan Duursma. Evaluation codes from smooth quadric surfaces and twisted Segre varieties. Designs, Codes and Cryptography, 2013, 66 (1-3), pp.291-303. 10.1007/s10623-012-9692-4 . hal-00707540

HAL Id: hal-00707540

https://inria.hal.science/hal-00707540v1

Submitted on 12 Jun 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Evaluation codes from smooth quadric surfaces and twisted Segre varieties

Alain Couvreur*and Iwan Duursma†

May 15, 2012

Abstract

We give the parameters of any evaluation code on a smooth quadric surface. For hyperbolic quadrics the approach uses elementary results on product codes and the parameters of codes on elliptic quadrics are obtained by detecting a BCH structure on these codes and using the BCH bound. The elliptic quadric is a twist of the surface $\mathbf{P}^1 \times \mathbf{P}^1$ and we detect a similar BCH structure on twists of the Segre embedding of a product of any d copies of the projective line.

Keywords: Evaluation codes, Algebraic Geometry codes, quadric surfaces, BCH codes, Segre embedding.

MSC: 94B27, 14J20, 94B15.

Introduction

The parameters of evaluation codes on quadric surfaces have been studied by Aubry (who also considered higher dimensional quadrics) in [1] and by Edoukou in [4]. Most of the results on the topic concern the evaluation of forms of degree one or two. The reason of this restriction is that the estimate of the minimum distance of such codes by geometric methods becomes harder when the degree increases.

In this article, we give the parameters of all evaluation codes on smooth quadric surfaces. The approach is not based on point counting but on the detection of a particular structure on the codes. Namely, we prove that codes on hyperbolic quadrics are tensor products of two extended Reed–Solomon codes and that codes on elliptic quadrics are extensions of some BCH codes studied by Pellikaan and the second author in [3]. A nice consequence of these results is that they solve a point counting problem which was not proved up to now. It should be underlined that usually, one tries to estimate the parameters of an Algebraic Geometry code by solving some equivalent geometric problem. In the present paper we proceed in the opposite direction. Namely, we are able to solve open geometric problems using known coding theoretic results.

Basically, studying codes on hyperbolic and elliptic quadrics reduces to study codes on $\mathbf{P}^1 \times \mathbf{P}^1$ and a twist of it. This approach has a natural generalisation to products of $d \geq 2$ copies of $\mathbf{P}^1$ yielding naturally tensor products of d extended Reed–Solomon codes and their twists yielding extended BCH codes of length $q^d + 1$. In particular, this construction gives a geometric realisation of a large class of BCH codes as evaluation codes and without using a subfield subcode operation.

The paper is organised as follows. The prerequisites on evaluation codes, twists and quadric surfaces are given in Section 1. Evaluation codes on hyperbolic quadric surfaces are considered in Section 2 and codes on elliptic quadrics are treated in Section 3. The higher dimensional case is studied in Section 4.

*Université Bordeaux I – Institut de Mathématiques de Bordeaux
†University of Illinois at Urbana-Champaign – Department of Mathematics

1 Prerequisites

1.1 Evaluation codes

Consider the projective space $\mathbf{P}^r_{\mathbf{F}_q}$ with its coordinate ring $\mathbf{F}_q[x_0, \ldots, x_r]$. For an integer s, denote by $\mathcal{F}_r(s)$ the space of homogeneous forms of degree s in $r+1$ variables, i.e. the space $H^0(\mathbf{P}^r, \mathcal{O}_{\mathbf{P}^r}(s))$. Given $f \in \mathcal{F}_r(s)$ and P a point of $\mathbf{P}^r$, we define the *evaluation* of f at P as $f(P) := f(p_0, \ldots, p_r)$, where $(p_0 : \ldots : p_r)$ is the system of homogeneous coordinates of P such that the first nonzero coordinate starting from the left is set to 1, i.e. is of the form $(0 : \ldots : 0 : 1 : p_i : \ldots : p_r)$.

Definition 1.1. Let $X \subset \mathbf{P}^r$ be a smooth projective variety over $\mathbf{F}_q$. The evaluation code $C_X(s)$ is defined as the image of the evaluation map

$$ev : \left\{ \begin{array}{ccc} \mathcal{F}_r(s) & \longrightarrow & \mathbf{F}_q^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)) \end{array} \right. ,$$

where $P_1, \ldots, P_n$ are the $\mathbf{F}_q$–points of X.

If we denote by $I_X(s)$ the degree s part of the homogeneous ideal $I_X \subset \mathbf{F}_q[x_0, \ldots, x_r]$ associated to X, then the above map ev obviously factors as $ev : \mathcal{F}_r(s)/I_X(s) \longrightarrow \mathbf{F}_q^n$.

The codes $C_X(s)$ for $X = \mathbf{P}^r$ are the projective Reed-Muller codes $PC_s(r, q)$ whose parameters were obtained by Sørensen [12, Theorem 1]. In this paper, we first consider the case that $X \subset \mathbf{P}^3$ is a smooth quadric. The case of a hyperbolic quadric corresponds to the Segre embedding of $\mathbf{P}^1 \times \mathbf{P}^1$ in $\mathbf{P}^3$ and the case of an elliptic quadric to a twist of such an embedding. We will then consider more generally the case that X is the Segre embedding of the product $\mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \hookrightarrow \mathbf{P}^{2^d-1}$ of d copies of the projective line, or a twist of such an embedding.

1.2 Twists

Given two varieties X and Y over a field k, one says that Y is a twist of X if the two varieties are not isomorphic as k–varieties but are as K–varieties, where K is a finite extension of k. For instance, the plane curves over $\mathbf{Q}$ defined by the homogeneous equations $x^2 + y^2 - z^2 = 0$ and $x^2 + y^2 + z^2 = 0$ are $\mathbf{Q}(\sqrt{-1})$–isomorphic but not $\mathbf{Q}$–isomorphic.

1.3 Smooth quadric surfaces

1.3.1 Elliptic and hyperbolic quadrics

Over a finite field $\mathbf{F}_q$ there exist two distinct isomorphism classes of smooth quadric surfaces, respectively called *elliptic quadrics* and *hyperbolic quadrics*. In $\mathbf{P}^3$, a hyperbolic quadric is projectively equivalent to the surface of equation

$$x_0x_3 - x_1x_2 = 0. \tag{1}$$

Given an irreducible homogeneous polynomial $Q(x, y)$ of degree two over $\mathbf{F}_q$, then any elliptic quadric is projectively equivalent to the surface of equation

$$x_0x_3 - Q(x_1, x_2) = 0. \tag{2}$$

We refer the reader to [8] for further details on these surfaces.

Remark 1.2. One can easily prove that the elliptic quadric is a twist of the hyperbolic one. Let $(x + wy)(x + w^q y)$ be the factorisation of Q over $\mathbf{F}_{q^2}$ (with $w \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$). The $\mathbf{F}_{q^2}$–linear automorphism of $\mathbf{P}^3$

$$\mu_{tw} : P \longmapsto AP, \qquad A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \omega & 0 \\ 0 & 1 & \omega^q & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3}$$

induces an $\mathbf{F}_{q^2}$–isomorphism between the elliptic and the hyperbolic quadric.

1.3.2 Rational parametrisation of quadrics.

Elliptic and hyperbolic quadrics are both rational. Here is a birational map from $\mathbf{P}^2$ to the hyperbolic quadric defined in (1).

$$\left\{ \begin{array}{ccc} \mathbf{P}^2 & \dashrightarrow & \mathbf{P}^3 \\ (x:y:z) & \longmapsto & (z^2 : xz : yz : xy) \end{array} \right. . \tag{4}$$

Here is a birational map from $\mathbf{P}^2$ to the elliptic quadric defined in (2).

$$\left\{ \begin{array}{ccc} \mathbf{P}^2 & \dashrightarrow & \mathbf{P}^3 \\ (x:y:z) & \longmapsto & (z^2 : xz : yz : Q(x,y)) \end{array} \right. . \tag{5}$$

Remark 1.3. The map (4) is regular on $\mathbf{P}^2 \setminus \{(1:0:0),(0:1:0)\}$. Denote by C the subvariety $\mathcal{H} \cap \{x_0 = 0\}$, then the image of the map (4) is $(\mathcal{H} \setminus C) \cup \{(0:0:0:1)\}$.

Remark 1.4. Let P be the closed point of degree 2 of $\mathbf{P}^2$ defined by

$$\{P\} = \{z = 0\} \cap \{Q(x,y) = 0\},$$

then the map (5) is regular on $\mathbf{P}^2 \setminus \{P\}$. It is in particular regular at all the $\mathbf{F}_q$–rational points of $\mathbf{P}^2$. Denote by C the subvariety $\mathcal{E} \cap \{x_0 = 0\}$, then the image of the map (4) is $(\mathcal{E} \setminus C) \cup \{(0:0:0:1)\}$. It is worth noting that the unique $\mathbf{F}_q$–rational point of C is $(0:0:0:1)$. Thus, the image of the map (5) contains all the rational points of $\mathcal{E}$.

2 Codes from hyperbolic quadrics

From now on, the hyperbolic quadric is denoted by $\mathcal{H}$. It is well–known that $\mathcal{H}$ is isomorphic to $\mathbf{P}^1 \times \mathbf{P}^1$. Indeed, the quadric $\mathcal{H}$ with equation $x_0x_3 - x_1x_2 = 0$ is the image of the Segre embedding (see [5, Chapter 4 §4], [11, Chapter I §5.1]):

$$\phi_s : \left\{ \begin{array}{ccc} \mathbf{P}^1 \times \mathbf{P}^1 & \longrightarrow & \mathbf{P}^3 \\ ((u_0:v_0),(u_1:v_1)) & \longmapsto & (u_0u_1 : u_0v_1 : v_0u_1 : v_0v_1) \end{array} \right. . \tag{6}$$

A homogeneous form $f \in \mathcal{F}_3(s)$ pulled back by ϕ yields the bi-homogeneous form $f(u_0u_1, u_0v_1, v_0u_1, v_0v_1)$ of bi-degree (s,s). Afterwards, one sees easily that the pullback map $\phi^\star$ induces an isomorphism $\mathcal{F}_3(s)/I_{\mathcal{H}}(s) \xrightarrow{\sim} \mathcal{F}_1(s) \otimes \mathcal{F}_1(s)$, where $I_{\mathcal{H}}(s)$ is the degree s part of the homogeneous ideal associated to $\mathcal{H}$. Consequently, the code $C_{\mathcal{H}}(s)$ is nothing but the code $C_{\mathbf{P}^1}(s) \otimes C_{\mathbf{P}^1}(s)$. The code $C_{\mathbf{P}^1}(s)$ is an extended Reed–Solomon code with parameters $[(q+1),(s+1),q-s+1]$. It is well–known that the minimum distance of a tensor product of two codes is the product of the minimum distances. This yields the following result.

Theorem 2.1. *Let $\mathcal{H}$ be a hyperbolic quadric over $\mathbf{F}_q$, let s be an integer such that $s < q$, then the code $C_{\mathcal{H}}(s)$ has parameters $[(q+1)^2,(s+1)^2,(q-s+1)^2]$.*

Remark 2.2. The above result is already partially proved by S.H. Hansen in [7, Example 3.2], where the author obtains $(q-s+1)^2$ as a lower bound for the minimum distance without proving that it is reached.

Actually, Hansen considers more general evaluation codes on $\mathcal{H}$: the codes obtained by evaluating spaces of forms whose pullback by ϕ are of the form $\mathcal{F}_1(a) \otimes \mathcal{F}_1(b)$. Using the above approach, one proves easily that such codes have parameters $[(q+1)^2,(a+1)(b+1),(q-a+1)(q-b+1)]$. This proves that the lower bound of Hansen is the actual minimum distance.

Remark 2.3. For $s = 2$, the result has been proved in [4, Theorem 6.2].

Remark 2.4. Using the structure of the Picard group of $\mathcal{H}$, one can prove that any evaluation code on $\mathcal{H}$ is equivalent to one of the codes described in Remark 2.2. Therefore, using Remark 2.2, we have the exact parameters of any evaluation code on $\mathcal{H}$.

Theorem 2.1 has the following geometric corollary.

Corollary 2.5 (Maximum number of points of an (s,s)–curve)**.** *Let X be a curve obtained by the intersection of $\mathcal{H}$ with a surface of degree s of $\mathbf{P}^3$ which does not contain $\mathcal{H}$. Then, the number of rational points of X satisfies*

$$\sharp X(\mathbf{F}_q) \leq 2s(q+1) - s^2$$

and the equality holds if and only if X is a union of s lines of the form $\phi(\{a\} \times \mathbf{P}^1)$ and s lines of the form $\phi(\mathbf{P}^1 \times \{b\})$.

Proof. The upper bound comes from Theorem 2.1. Moreover, it is easy to see that the union of s rational lines of the first ruling and s lines of the other one has $2s(q+1) - s^2$ rational points.

Conversely, it is well–known that the minimum weight codewords of a tensor product of codes are tensor products of minimum weight codewords. Thus, minimum weight codewords of $C_{\mathcal{H}}(s)$ are obtained by the evaluation of forms f whose pullback $\phi^\star f$ equals $g(u_0,v_0)h(u_1,v_1)$, where g,h both split in products of s distinct polynomials of degree one. Thus, the vanishing locus of f is a union of lines and any f whose vanishing locus is not such a union has strictly less rational points in its vanishing locus on $\mathcal{H}$. □

About the geometry of the minimum weight codewords of $C_{\mathcal{H}}(s)$

In Corollary 2.5, one can prove easily that if $\sharp X(\mathbf{F}_q) = 2s(q+1) - s^2$, then, one of the surfaces $\mathcal{S}$ of degree s such that $\mathcal{S} \cap \mathcal{H} = X$ is a union of s distinct planes such that each one of them is tangent to $\mathcal{H}$ at some rational point. This claim generalises [4, Theorem 6.3], which treats the case $s = 2$.

Remark 2.6. In [4, Theorem 6.3], the author asserts that if $X = \mathcal{H} \cap \mathcal{S}$, with $\mathcal{S}$ a quadric, has $4q$ rational points, then $\mathcal{S}$ is either a pair of planes or another hyperbolic quadric with 4 common lines with $\mathcal{H}$. Actually, the set of quadrics $\mathcal{S}$ such that $\mathcal{S} \cap \mathcal{H} = X$ is a linear system of dimension 1 which always contains a pair of planes.

3 BCH codes and codes on elliptic quadrics

From now on, the elliptic quadric is denoted by $\mathcal{E}$ and s denotes a positive integer. The aim of this section is to prove that the codes $C_{\mathcal{E}}(s)$ are extended BCH codes. More precisely, these codes of length q^2+1 (the elliptic quadric has q^2+1 rational points, see [8, Table IV.15.4]) punctured at two positions yield BCH codes of length q^2-1.

3.1 The cyclic structure

The cyclic structure of the punctured codes can be explained geometrically. Indeed, the automorphism group of the elliptic quadric contains an element fixing two rational points and shifting cyclically the q^2-1 other ones.

Let us describe such an automorphism. Consider the description of $\mathcal{E}$ given in (2) and assume moreover that w is a primitive element of $\mathbf{F}_{q^2}/\mathbf{F}_q$. The multiplication by w in $\mathbf{F}_{q^2}$ provides an automorphism $\sigma_w \in \mathbf{Aut}_{\mathbf{F}_q}(\mathbf{A}^2)$ which extends to $\mathbf{Aut}_{\mathbf{F}_q}(\mathbf{P}^2)$ and, thanks to the parametrisation map (5), yields an automorphism $\tilde{\sigma}_w \in \mathbf{Aut}_{\mathbf{F}_q}(\mathcal{E})$. The map $\tilde{\sigma}_w$ is the restriction to $\mathcal{E}$ of a linear automorphism of $\mathbf{P}^3$ described by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -N(w) & 0 \\ 0 & 1 & Tr(w) & 0 \\ 0 & 0 & 0 & N(w) \end{pmatrix},$$

where $N(w)$ and $Tr(w)$ denote respectively the norm $N(w) := w^{q+1}$ and the trace $Tr(w) := w + w^q$. One can check that this automorphism fixes the points $(1:0:0:0)$ and $(0:0:0:1)$ and shifts cyclically the q^2-1 other rational points of $\mathcal{E}$.

3.2 A class of BCH codes

3.2.1 The cyclic codes

Definition 3.1. For a given field $\mathbf{F}_q$ and a positive integer $s < q$, let $B(s)$ be the cyclic code defined over the extension field $\mathbf{F}_{q^2}$ which is generated by the vectors of the form $(\zeta^r | \zeta \in \mathbf{F}_{q^2}^\times)$, for $r = i + qj$ such that $0 \leq i, j \leq s$. In addition, let $B_0(s)$ be the subfield subcode $B(s)_{|\mathbf{F}_q}$.

This class of codes is studied in [3] where the following result is proved.

Proposition 3.2. *The code $B_0(s)$ has parameters $[q^2 - 1, (s+1)^2, q^2 - 1 - s(q+1)]$. Moreover it is a BCH code.*

Proof. [3, Proposition 12]. □

Remark 3.3. The condition $0 \leq i, j \leq s$ differs from the condition $0 \leq i + j \leq s$ that is used to describe punctured Reed-Muller codes as cyclic codes.

3.2.2 The extended BCH codes

Actually the codes from elliptic quadrics are related to some extended version of the above described BCH codes. Thus, we introduce a new class of codes.

Definition 3.4. Consider the projective line $\mathbf{P}^1$ over $\mathbf{F}_{q^2}$ and let $0 \leq s \leq q-1$ be an integer. We denote by $B^{ext}(s)$ the subcode of $C_{\mathbf{P}^1}(s(q+1))$ spanned by the evaluation at $\mathbf{P}^1(\mathbf{F}_{q^2})$ of the forms

$$x^{i+qj} y^{s-i+q(s-j)}, \qquad 0 \leq i, j \leq s.$$

The extended BCH code $B_0^{ext}(s)$ is defined as the subfield subcode $B^{ext}(s)_{|\mathbf{F}_q}$.

Remark 3.5. Clearly, $B(s)$ and $B_0(s)$ can be respectively obtained by puncturing $B^{ext}(s)$ and $B_0^{ext}(s)$ at the positions corresponding to $(0:1)$ and $(1:0)$.

Remark 3.6. An interesting feature of the codes $B_0^{ext}(s)$ compared to $B_0(s)$ is that they have a large permutation group. Indeed, the group $PSL(2, \mathbf{F}_{q^2})$ acts on $B^{ext}(s)$ and $B_0^{ext}(s)$ by permutation. In particular, these codes are 3–transitive.

Proposition 3.7. *For $0 \leq s \leq q-2$, the code $B_0^{ext}(s)$ has parameters $[q^2+1, (s+1)^2, q^2+1-s(q+1)]$.*

Proof. The length is obvious. For the dimension, let us prove that the puncturing map $p : B_0^{ext}(s) \longrightarrow B_0(s)$ evoked in Remark 3.5 is injective. Denote respectively by P_0 and P_∞ the points $(0:1)$ and $(1:0)$ of $\mathbf{P}^1$. The kernel of p is the subspace of codewords of $B_0^{ext}(s)$ with supports contained in $\{P_0, P_\infty\}$. If such a nonzero word exists, then from Remark 3.6, there exists a word of weight ≤ 2 whose support avoids P_0 and P_∞. By puncturing, this would yield a codeword of weight ≤ 2 in $B_0(s)$, which contradicts Proposition 3.2.

For the minimum distance, using Proposition 3.2 and Remark 3.5 we know that the minimum distance d of $B_0^{ext}(s)$ satisfies

$$d \leq q^2 + 1 - s(q+1). \tag{7}$$

Take a codeword $w \in B_0^{ext}(s)$ of minimum weight d. Using Remark 3.6, one can assume that P_0 and P_∞ are contained in the support of w. The punctured codeword $p(w) \in B_0(s)$ has weight $d-2$ and from Proposition 3.2, we have $d - 2 \geq q^2 - 1 - s(q+1)$. This inequality together with (7) yield the result. □

3.3 A twisted embedding of the projective line

The elliptic quadric $\mathcal{E} \subset \mathbf{P}^3$ over $\mathbf{F}_q$ contains q^2+1 rational points. Using (5) together with Remark 1.4 they are described by

$$\mathcal{P} = \{(1 : u : v : Q(u,v)) : u, v \in \mathbf{F}_q\} \cup \{(0:0:0:1)\}, \tag{8}$$

where $Q(u,v) = (u + \omega v)(u + \omega^q v)$ as in (5).

Set

$$\phi_f : \left\{ \begin{array}{ccc} \mathbf{P}^1 & \longrightarrow & \mathbf{P}^1 \times \mathbf{P}^1 \\ (x:y) & \longmapsto & ((x:y),(x^q:y^q)) \end{array} \right. . \tag{9}$$

Consider the $\mathbf{F}_q$–embedding

$$\psi : \left\{ \begin{array}{ccccc} \mathbf{P}^1 & \xrightarrow{\phi_f} & \mathbf{P}^1 \times \mathbf{P}^1 & \xrightarrow{\phi_s} & \mathbf{P}^3 \\ (x:y) & \longmapsto & ((x:y),(x^q:y^q)) & \longmapsto & (y^{q+1} : xy^q : x^q y : x^{q+1}) \end{array} \right. , \tag{10}$$

where ϕ_f is defined in (9) and ϕ_s is the Segre embedding (6). Over $\mathbf{F}_{q^2}$, the projective line has q^2+1 rational points $\{(x:1) : x \in \mathbf{F}_{q^2}\} \cup (1:0)$. Writing $x = u + \omega v$, for $u, v \in \mathbf{F}_q$, their images in $\mathbf{P}^3$ by the map (10) are

$$\mathcal{P}' = \{(1 : u + \omega v : u + \omega^q v : Q(u,v)) : u, v \in \mathbf{F}_q\} \cup \{(0:0:0:1)\}. \tag{11}$$

Clearly, a point $P' \in \mathcal{P}'$ differs from a point $P \in \mathcal{P}$ by the linear transformation μ_{tw} of (3). Consequently, we state the following lemma.

Lemma 3.8. *We have an $\mathbf{F}_{q^2}$–embedding of $\mathbf{P}^1$*

$$\psi_{tw} := \mu_{tw}^{-1} \circ \psi : \mathbf{P}^1 \xrightarrow{\phi_f} \mathbf{P}^1 \times \mathbf{P}^1 \xrightarrow{\phi_s} \mathbf{P}^3 \xrightarrow{\mu_{tw}^{-1}} \mathbf{P}^3 \tag{12}$$

inducing a one-to-one map $\mathbf{P}^1(\mathbf{F}_{q^2}) \longrightarrow \mathcal{E}(\mathbf{F}_q)$.

Thanks to the $\mathbf{F}_{q^2}$–embedding ψ_{tw}, the $\mathbf{F}_{q^2}$–codes $C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}$ can be regarded as codes over $\mathbf{P}^1$. This is the key point of the proof of the equality $C_{\mathcal{E}}(s) = B_0^{ext}(s)$ (up to a permutation) established in the following subsection.

3.4 The parameters of the codes on the elliptic quadric

The objective is to determine the parameters and in particular the minimum distance of the codes $C_{\mathcal{E}}(s)$. This objective is reached by Theorem 3.10. Recall that except for the case $s = 1, 2$, the minimum distance of these codes was unknown up to now.

For the proof of Theorem 3.10 we need the following combinatorial lemma.

Lemma 3.9. *The sets of pairs of integers $U^{(s)} = \{(i+k, j+k) : 0 \le i, j, k$ and $i+j+k \le s\}$ and $V^{(s)} = \{(i,j) : 0 \le i, j \le s\}$ are equal.*

Proof. Clearly $U^{(s)} \subset V^{(s)}$. Conversely, for $(i,j) \in V^{(s)}$ and for $k = \min\{i,j\}$, we have $(i,j) = ((i-k)+k, (j-k)+k) \in U^{(s)}$. □

Theorem 3.10. *The code $C_{\mathcal{E}}(s)$ is permutation equivalent to the extended BCH code $B_0^{ext}(s)$ introduced in Definition 3.1. Therefore, for all $0 \le s < q-1$, the code $C_{\mathcal{E}}(s)$ has parameters $[q^2+1, (s+1)^2, q^2+1-s(q+1)]$.*

Proof. The code $C_{\mathcal{E}}(s)$, which is defined over $\mathbf{F}_q$, and the code $C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}$, which has coefficients over $\mathbf{F}_{q^2}$, use the same generator matrix and have the same parameters.

Clearly, the subfield subcode $(C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2})_{|\mathbf{F}_q}$ equals $C_{\mathcal{E}}(s)$. Thus, to prove that $C_{\mathcal{E}}(s) = B_0^{ext}(s)$, it is sufficient to prove that $C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2} = B^{ext}(s)$ (see Definition 3.4). Afterwards, the parameters of $C_{\mathcal{E}}(s)$ are given by Proposition 3.7.

Step 1. We first prove that $C_{\mathcal{E}}(1) \otimes \mathbf{F}_{q^2} = B^{ext}(1)$. The code $C_{\mathcal{E}}(1) \otimes \mathbf{F}_{q^2}$ is obtained by evaluating $\mathcal{F}_3(1) \otimes \mathbf{F}_{q^2}$ at the set $\mathcal{P}$ described in (8).

Because of the bijection induced by ψ_{tw} in Lemma 3.8 between the $\mathbf{F}_q$–rational points of $\mathcal{E}$ and the $\mathbf{F}_{q^2}$–rational points of $\mathbf{P}^1$, the code can equivalently be obtained by evaluating the pullbacks $\psi_{tw}^\star(\mathcal{F}_3(1) \otimes \mathbf{F}_{q^2})$ at the elements of $\mathbf{P}^1(\mathbf{F}_{q^2})$.

Recall that, from §3.3, we have $\psi_{tw} = \mu_{tw}^{-1} \circ \phi$, where μ_{tw} and ψ are respectively defined in (3) and (10). Since μ_{tw} is $\mathbf{F}_{q^2}$–linear, one sees easily that $(\mu_{tw}^{-1})^\star(\mathcal{F}_3(1) \otimes \mathbf{F}_{q^2}) = \mathcal{F}_3(1) \otimes \mathbf{F}_{q^2}$ and hence $\psi_{tw}^\star(\mathcal{F}_3(1) \otimes \mathbf{F}_{q^2}) = \psi^\star(\mathcal{F}_3(1) \otimes \mathbf{F}_{q^2})$. Finally, (10) entails that $\psi^\star(\mathcal{F}_3(1) \otimes \mathbf{F}_{q^2})$ is generated by $y^{q+1}, xy^q, x^q y, x^{q+1}$. Evaluating these forms at $\mathbf{P}^1(\mathbf{F}_{q^2})$ yields $B^{ext}(1)$ (see Definition 3.4).

Step 2. For the general case we just copy Step 1. By the same manner $C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}$ can be obtained by evaluating the elements of $\psi^{\star}_{tw}(\mathcal{F}_3(s) \otimes \mathbf{F}_{q^2})$ at the elements of $\mathbf{P}^1(\mathbf{F}_q)$. In addition, one proves, as in Step 1, that $\psi^{\star}_{tw}(\mathcal{F}_3(s) \otimes \mathbf{F}_{q^2}) = \psi^{\star}(\mathcal{F}_3(s) \otimes \mathbf{F}_{q^2})$.

The space $\psi^{\star}(\mathcal{F}_3(s) \otimes \mathbf{F}_{q^2})$ is generated by monomials of degree s in y^{q+1}, xy^q, $x^q y, x^{q+1}$. Such a monomial is of the form

$$y^{a(q+1)}(xy^q)^b(x^q y)^c x^{d(q+1)} = x^{(b+d)+q(c+d)} y^{(a+c)+q(a+b)}, \quad \text{for } a+b+c+d = s.$$

From Lemma 3.9, this set of monomials equals

$$\left\{ x^{(i+qj)} y^{(s-i)+q(s-j)} \mid 0 \leq i, j \leq s \right\},$$

which yields the result by definition of $B^{ext}(s)$. □

Remark 3.11. It is worth noting that the above proof points out a very interesting property of $B(s)$. Indeed, even if $B(s)$ is defined over $\mathbf{F}_{q^2}$, it is generated by words defined over $\mathbf{F}_q$. Thus, the $\mathbf{F}_q$–dimension of its subfield subcode $B_0(s)$ equals the $\mathbf{F}_{q^2}$–dimension of $B(s)$. This explains why the codes $B_0(s)$ provide many of the best known codes (see [6]): in general the subfield subcode operation entails a dramatic reduction of the dimension. This reduction does not happen for the codes $B(s)$.

Remark 3.12. Since the Picard group of $\mathcal{E}$ is generated by $\mathcal{O}_{\mathcal{E}}(1)$, any evaluation code on this surface is equivalent to $C_{\mathcal{E}}(s)$ for some s. Thus, as for the hyperbolic quadric, we have here the exact parameters of any evaluation code on $\mathcal{E}$.

Theorem 3.10 has a geometric corollary.

Corollary 3.13. *Let $s < q-1$. Let $X \subset \mathcal{E}$ be a curve obtained by the intersection of $\mathcal{E}$ with a surface of degree s which does not contain $\mathcal{E}$. Then,*

$$\sharp X(\mathbf{F}_q) \leq s(q+1).$$

Proof. It is a straightforward consequence of Theorem 3.10. □

About the geometry of the minimum weight codewords of $C_{\mathcal{E}}(s)$

Comparing Corollary 3.13 with Corollary 2.5, it is natural to ask: *If equality holds in Corollary 3.13, is the curve X a cut out of $\mathcal{E}$ by s planes?*

Consider s distinct planes $\Pi_1, \ldots, \Pi_s$ non tangent to $\mathcal{E}$ and such that for all i, j, the line $\Pi_i \cap \Pi_j$ does not meet $\mathcal{E}$ at rational points and set $\mathcal{S} := \Pi_1 \cup \ldots \cup \Pi_s$. Clearly, the curve $X := \mathcal{S} \cap \mathcal{E}$ has $s(q+1)$ rational points. Conversely, if $s = 1, 2$, the curves reaching this upper bound are always cut outs by s planes. The claim is elementary for $s = 1$ and the case $s = 2$ is treated in [4, Theorem 6.9] (an argument similar to that of Remark 2.6 leads to this conclusion). However, for $s \geq 3$, there exist curves reaching this bound but which are not cut outs by planes, some of them are actually irreducible. Computer aided calculations using the software Magma [2] provided the following example.

Example 3.14. Let $s = 3$ and $q = 5$. The surface $\mathcal{E}$ is defined by the equation $3y^2 + 3yz + z^2 + 4xt = 0$. Let $\mathcal{S}$ be the surface of equation

$$(\mathcal{S}) \qquad 3x^3 + 2x^2y + 2xy^2 + 3x^2z + 4xyz + 3y^2z + 2x^2t + 2xyt + 4xzt + 4yzt + xt^2 + 3yt^2 + 2zt^2 = 0,$$

then the curve $X = \mathcal{E} \cap \mathcal{S}$ is irreducible and has $18 = 3(5+1)$ rational points.

4 Higher dimensional analogues

The results in the previous sections give us the actual parameters of evaluation codes on smooth quadric surfaces. The case of a hyperbolic quadric was proved by establishing a relation with tensored Reed-Solomon codes and the case of an elliptic quadric was proved using a correspondence with a suitable class of BCH codes. The hyperbolic quadric is the image $\mathcal{H}$ of $\mathbf{P}^1 \times \mathbf{P}^1$ in $\mathbf{P}^3$ under the Segre embedding and the elliptic quadric $\mathcal{E}$ is a quadratic twist of this embedding. Both embeddings generalise and in this section we will describe evaluation codes defined on the image $\mathcal{H} \subset \mathbf{P}^{2^d-1}$ of the Segre embedding $\phi : \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \longrightarrow \mathbf{P}^{2^d-1}$ of d copies of $\mathbf{P}^1$ and on twists $\mathcal{E}$ of $\mathcal{H}$.

4.1 The non-twisted case

Let $\mathcal{H} \subset \mathbf{P}^{2^d-1}$ be the Segre embedding of d copies of $\mathbf{P}^1$ and let $I_{\mathcal{H}} \subset \mathbf{F}_r$ be its associated homogeneous ideal. As in (6) denote by ϕ_s the Segre's embedding. Similar to the case of the hyperbolic quadric, the pullback map $\phi_s^\star$ induces an isomorphism $\mathcal{F}_d(s)/I_{\mathcal{H}}(s) \xrightarrow{\sim} \mathcal{F}_1(s) \otimes \cdots \otimes \mathcal{F}_1(s)$ (d copies). Consequently, the evaluation code $C_{\mathcal{H}}(s)$ over $\mathbf{F}_q$ with $s < q$ can be described as a tensor product $C_{\mathbf{P}^1}(s) \otimes C_{\mathbf{P}^1}(s)$ of extended Reed-Solomon codes.

Theorem 4.1. *Let $\mathcal{H}$ be the Segre embedding of the product $\mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \hookrightarrow \mathbf{P}^{2^d-1}$ of d copies of projective line over $\mathbf{F}_q$, let s be an integer such that $s < q$, then the code $C_{\mathcal{H}}(s)$ has parameters $[(q+1)^d, (s+1)^d, (q-s+1)^d]$. Moreover, the code is the d-fold tensor product of an extended Reed-Solomon code.*

It is well–known that the homogeneous ideal $I_{\mathcal{H}} \subset \mathcal{F}_{2^d-1} = \mathbf{F}_q[x_0, \ldots, x_r]$ for $\mathcal{H}$ is generated by quadrics. In fact this is true more generally for the larger class of Segre embeddings of projective space of any dimension (details and further references can be found in [10]). The Segre embedding $\mathcal{H}$ of $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$ in $\mathbf{P}^7$ is the intersection of nine quadrics. Here is a birational map from $\mathbf{P}^3$ to $\mathcal{H}$.

$$\left\{ \begin{array}{ccc} \mathbf{P}^3 & \dashrightarrow & \mathbf{P}^7 \\ (t:x:y:z) & \longmapsto & (t^3 : t^2x : t^2y : t^2z : txy : tyz : tzx : xyz) \end{array} \right. \tag{13}$$

The nine quadrics that define $\mathcal{H}$ correspond to the relations $(t^2x)(t^2y) = (t^3)(txy)$, $(t^2x)(tyz) = (t^3)(xyz)$, $(t^2x)(xyz) = (txy)(tzx)$ and their cyclic permutations under $x \longmapsto y \longmapsto z \longmapsto x$. The full resolution, given in [9], is

$$0 \longrightarrow \mathcal{F}_7[-6] \longrightarrow \mathcal{F}_7[-4]^9 \longrightarrow \mathcal{F}_7[-3]^{16} \longrightarrow \mathcal{F}_7[-2]^9 \longrightarrow \mathcal{F}_7 \longrightarrow \mathcal{F}_7/I_{\mathcal{H}} \longrightarrow 0.$$

4.2 The twisted case

We will first define the twisted variety $\mathcal{E}$ of $\mathcal{H}$, for $\mathcal{H}$ the Segre embedding of d copies of $\mathbf{P}^1$. We will then show how similar to the case $d = 2$ the $q^d + 1$ rational points $\mathcal{E}(\mathbf{F}_q)$ are in bijection with the $q^d + 1$ rational points $\mathbf{P}^1(\mathbf{F}_{q^d})$. Finally this allows us to interpret the evaluation codes $C_{\mathcal{E}}(s)$ as extended BCH codes. Set $r := 2^d - 1$. For $d \geq 2$, let $\phi : \mathbf{P}^d \dashrightarrow \mathbf{P}^r$ be the natural rational map with image in $\mathcal{H} \subset \mathbf{P}^r$. The special case $d = 3$ is given by (13).

Definition 4.2. For $d \geq 2$, let $(x_0 : x_1 : \cdots : x_d)$ be coordinates for $\mathbf{P}^d$, let $\alpha_1, \ldots, \alpha_d$ be an $\mathbf{F}_q$–basis of $\mathbf{F}_{q^d}$ and let

$$\lambda : \left\{ \begin{array}{ccc} \mathbf{P}^d & \longrightarrow & \mathbf{P}^d \\ (x'_0 : x'_1 : \ldots : x'_d) & \longmapsto & (x_0 : x_1 : \ldots : x_d) \end{array} \right.$$

be the $\mathbf{F}_{q^d}$-linear transformation

$$\left\{ \begin{array}{lcl} x_0 & := & x'_0 \\ x_j & := & \alpha_1^{q^{j-1}} x'_1 + \cdots + \alpha_d^{q^{j-1}} x'_d, \quad \text{for } j \in \{1, \ldots, d\} \end{array} \right. .$$

The rational map $\phi \circ \lambda : \mathbf{P}^d \dashrightarrow \mathbf{P}^r$ factors as $\mu_{tw} \circ \phi' : \mathbf{P}^d \dashrightarrow \mathbf{P}^r$ for a linear transformation $\mu_{tw} : \mathbf{P}^r \longrightarrow \mathbf{P}^r$ over $\mathbf{F}_{q^d}$ and a rational map $\phi' : \mathbf{P}^d \dashrightarrow \mathbf{P}^r$ over $\mathbf{F}_q$. The embedding ϕ' is called the twisted embedding with image $\mathcal{E}$.

We illustrate the twisted embeddings for the cases $d = 2$ and $d = 3$.

Example 4.3. For $d = 2$, the variety $\mathcal{H} \subset \mathbf{P}^3$. Over $\mathbf{F}_q$ it contains the rational points $(1 : x : y : xy)$, for $x, y \in \mathbf{F}_q$. For the twisted variety $\mathcal{E}$, let $\{b, b^q\}$ be a basis for $\mathbf{F}_{q^2}/\mathbf{F}_q$ and let

$$\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}, \qquad \text{for } A = \begin{pmatrix} b & b^q \\ b^q & b \end{pmatrix}.$$

Then

$$(1 : x : y : xy)^T = (I_1 \oplus A \oplus I_1)(1 : u : v : Q)^T,$$

for $xy = (bu + b^q v)(b^q u + bv) =: Q(u, v)$ irreducible of degree two over $\mathbf{F}_q$. The rational map ϕ' is given by

$$\phi' : \left\{ \begin{array}{ccc} \mathbf{P}^2 & \dashrightarrow & \mathbf{P}^3 \\ (1 : u : v) & \longmapsto & (1 : u : v : Q) \end{array} \right. . \tag{14}$$

The finite rational points on the image $\mathcal{E}$ correspond to $\{(1 : u : v : Q) : u, v \in \mathbf{F}_q\}$.

Example 4.4. For $d = 3$, the variety $\mathcal{H} \subset \mathbf{P}^7$. Over $\mathbf{F}_q$ it contains the rational points $(1 : x : y : z : xy : yz : zx : xyz)$ for $x, y, z \in \mathbf{F}_q$. For the twisted variety $\mathcal{E}$, let $\{c, c^q, c^{q^2}\}$ be a basis for $\mathbf{F}_{q^3}/\mathbf{F}_q$ and let

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} u \\ v \\ w \end{pmatrix}, \qquad \text{for } A = \begin{pmatrix} c & c^q & c^{q^2} \\ c^q & c^{q^2} & c \\ c^{q^2} & c & c^q \end{pmatrix}.$$

Then

$$(1 : x : y : z : xy : yz : zx : xyz)^T = (I_1 \oplus A \oplus B \oplus I_1)(1 : u : v : w : Q_1 : Q_2 : Q_3 : R)^T, \tag{15}$$

for $xyz =: R(u, v, w)$ irreducible of degree three over $\mathbf{F}_q$, and for a $\mathbf{F}_{q^d}$-linear transformation B and polynomials Q_1, Q_2, Q_3 of degree two over $\mathbf{F}_q$. The rational map ϕ' is given by

$$\phi' : \left\{ \begin{array}{ccc} \mathbf{P}^3 & \dashrightarrow & \mathbf{P}^7 \\ (1 : u : v : w) & \longmapsto & (1 : u : v : w : Q_1 : Q_2 : Q_3 : R) \end{array} \right. . \tag{16}$$

The finite rational points on the image $\mathcal{E}$ correspond to $\{(1 : u : v : w : Q_1 : Q_2 : Q_3 : R) : u, v, w \in \mathbf{F}_q\}$. A convenient choice for the polynomials Q_1, Q_2, Q_3 is as partial derivatives of the polynomial $R(u, v, w)$. The partial derivatives of $R(u, v, w)$ are defined over $\mathbf{F}_q$ and up to a linear transformation over $\mathbf{F}_{q^3}$ correspond to the partial derivatives of xyz. We include the details.

$$\begin{pmatrix} \partial/\partial_u \\ \partial/\partial_v \\ \partial/\partial_w \end{pmatrix} = A^T \begin{pmatrix} \partial/\partial_x \\ \partial/\partial_y \\ \partial/\partial_z \end{pmatrix}$$

In particular, for $xyz = R(u, v, w)$,

$$\begin{pmatrix} yz \\ zx \\ xy \end{pmatrix} = \begin{pmatrix} \partial/\partial_x \\ \partial/\partial_y \\ \partial/\partial_z \end{pmatrix} (xyz) = (A^T)^{-1} \begin{pmatrix} \partial/\partial_u \\ \partial/\partial_v \\ \partial/\partial_w \end{pmatrix} R(u, v, w).$$

For the variety $\mathcal{E}$ defined over $\mathbf{F}_q$ we obtain evaluation codes $C_{\mathcal{E}}(s)$ defined over $\mathbf{F}_q$. To determine the parameters of the codes we use a bijection between the rational points $\mathcal{E}(\mathbf{F}_q)$ and the rational points $\mathbf{P}^1(\mathbf{F}_{q^d})$ of the projective line over $\mathbf{F}_{q^d}$. In analogy with (10) consider the $\mathbf{F}_q$–embedding

$$\psi : \mathbf{P}^1 \xrightarrow{\phi_f} \mathbf{P}^1 \times \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \xrightarrow{\phi_s} \mathbf{P}^r, \tag{17}$$

where

$$\phi_f : \left\{ \begin{array}{ccc} \mathbf{P}^1 & \longrightarrow & \mathbf{P}^1 \times \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \\ (x : y) & \longmapsto & ((x : y), (x^q : y^q), \ldots (x^{q^{d-1}} : y^{q^{d-1}})) \end{array} \right. ,$$

and ϕ_s is the Segre embedding such that $\psi(x : y) = (y^{q^{d-1}+\cdots+q+1} : \cdots : x^{q^{d-1}+\cdots+q+1})$.

Lemma 4.5. *We have an $\mathbf{F}_{q^d}$–embedding of $\mathbf{P}^1$*

$$\psi_{tw} := \mu_{tw}^{-1} \circ \psi : \mathbf{P}^1 \xrightarrow{\phi_f} \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \xrightarrow{\phi_s} \mathbf{P}^r \xrightarrow{\mu_{tw}^{-1}} \mathbf{P}^r \tag{18}$$

inducing a one-to-one map $\mathbf{P}^1(\mathbf{F}_{q^d}) \longrightarrow \mathcal{E}(\mathbf{F}_q)$.

Proof. The proof is similar to the proof of Lemma 3.8. Let $(x : 1)$ be a finite rational point on the projective line over $\mathbf{F}_{q^d}$. If we write $(x : 1) = (\alpha_1 x'_1 + \cdots + \alpha_d x'_d : 1)$, with $x'_1, \ldots, x'_d \in \mathbf{F}_q$, for $\alpha_1, \ldots, \alpha_d$ as in Definition 4.2, then the image of $(x : 1)$ under ψ differs from a finite rational point in $\mathcal{E}(\mathbf{F}_q)$ by the linear transformation μ_{tw}. □

Definition 4.6. Consider the projective line $\mathbf{P}^1$ over $\mathbf{F}_{q^d}$ and let $0 \leq s \leq q-1$ be an integer. For $m = s(q^d-1)/(q-1)$, denote by $B^{ext}(s)$ the subcode of $C_{\mathbf{P}^1}(m)$ spanned by the evaluation at $\mathbf{P}^1(\mathbf{F}_{q^d})$ of the forms

$$\{x^i y^{m-i} : i = i_0 + i_1 q + \cdots + i_{d-1} q^{d-1} \text{ and } 0 \leq i_0, i_1, \ldots, i_{d-1} \leq s,\}. \tag{19}$$

The code $B_0^{ext}(s)$ is defined as the subfield subcode $B^{ext}(s)_{|\mathbf{F}_q}$.

The codes $B^{ext}(s)$ and $B_0^{ext}(s)$ admit the group $PSL(2, \mathbf{F}_{q^d})$ as a 3-transitive automorphism group. After puncturing at $(0:1)$ and $(1:0)$ the code $B_0^{ext}(s)$ is a BCH code of type $[q^d-1, (s+1)^d, q^d-1-m]$ ([3, Proposition 12]).

Theorem 4.7. *For all $s < q-1$, the code $C_{\mathcal{E}}(s)$ has parameters $[q^d+1, (s+1)^d, q^d+1-s(q^d-1)/(q-1)]$. Moreover, the code $C_{\mathcal{E}}(s)$ is permutation equivalent with an extended BCH code.*

Proof. The proof is similar to the proof of Theorem 3.10. Because of the bijection induced by ψ_{tw} in Lemma 4.5 between the $\mathbf{F}_q$–rational points of $\mathcal{E}$ and the $\mathbf{F}_{q^d}$–rational points of $\mathbf{P}^1$, the code $C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^d}$ can be obtained by evaluating the pullbacks $\psi_{tw}^{\star}(\mathcal{F}_r(s) \otimes \mathbf{F}_{q^d})$ at the elements of $\mathbf{P}^1(\mathbf{F}_{q^d})$. The linear transformation μ_{tw} does not affect the code over $\mathbf{F}_{q^d}$ and it suffices to consider the pullbacks $\psi^{\star}(\mathcal{F}_r(s) \otimes \mathbf{F}_{q^d})$. The definition of ψ in (17) entails that $\psi^{\star}(\mathcal{F}_r(s) \otimes \mathbf{F}_{q^d})$ is generated by forms $x^i y^{m-i}$ that, in affine form, are the product of s monomials chosen from

$$\{1^{j_0} x^{j_1} (x^q)^{j_2} \cdots (x^{q^{d-1}})^{j_{d-1}} : 0 \leq j_0, j_1, \ldots, j_{d-1} \leq 1\}. \tag{20}$$

Every such product is of the form (19). Conversely, each from in (19) can be written as a product of s monomials in (20). The latter is clear if for a given monomial $x^i y^{m-i}$ we use an ordering on $i_0, i_1, \ldots, i_{d-1}$ to choose the monomials needed for the product. Thus we have shown that $C_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^d}$ is the code $B(s)$ in Definition 4.6. This clearly implies that $C_{\mathcal{E}}(s)$ is permutation equivalent with the extended BCH code $B_0(s)$. Moreover, using the 3−transitivity of the automorphism group it implies that the parameters of $C_{\mathcal{E}}(s)$ are as claimed (as in the proof of Proposition 3.7). □

We observe that the last theorem has applications in two directions. It shows first that the maximum number of $\mathbf{F}_q$–rational zeros in $\mathcal{E} \subset \mathbf{P}^r$ of a homogeneous form of degree s agrees with the BCH bound, that is to say it can be obtained using fairly elementary coding theory and without using geometric tools. On the other hand it gives certain BCH codes a geometric interpretation as evaluation codes on an algebraic variety.

Acknowledgements.

The first author is supported by the French ANR Defis program under contract ANR-08-EMER-003 (COCQ project).

References

[1] Y. Aubry. Reed-Muller codes associated to projective algebraic varieties. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 4–17. Springer, Berlin, 1992.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] I. M. Duursma and R. Pellikaan. A symmetric Roos bound for linear codes. *J. Combin. Theory Ser. A*, 113(8):1677–1688, 2006.

[4] F. A. B. Edoukou. Codes defined by forms of degree 2 on quadric surfaces. *IEEE Trans. Inform. Theory*, 54(2):860–864, 2008.

[5] W. Fulton. *Algebraic curves.* Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989.

[6] M. Grassl. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2010-07-22.

[7] S. H. Hansen. Error-correcting codes from higher-dimensional varieties. *Finite Fields Appl.*, 7(4):531–552, 2001.

[8] J. W. P. Hirschfeld. *Finite projective spaces of three dimensions.* Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1985. Oxford Science Publications.

[9] E. Rubei. On syzygies of Segre embeddings. *Proc. Amer. Math. Soc.*, 130(12):3483–3493 (electronic), 2002.

[10] E. Rubei. Resolutions of Segre embeddings of projective spaces of any dimension. *J. Pure Appl. Algebra*, 208(1):29–37, 2007.

[11] I. R. Shafarevich. *Basic algebraic geometry. 1.* Springer-Verlag, Berlin, second edition, 1994.

[12] A. B. Sørensen. Projective Reed-Muller codes. *IEEE Trans. Inform. Theory*, 37(6):1567–1576, 1991.

Alain Couvreur
Institut de Mathématiques de Bordeaux
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex, France
`couvreur@math.u-bordeaux1.fr`

Iwan Duursma
Department of Mathematics
University of Illinois at Urbana–Champaign
1409 W. Green Street (MC-382)
Urbana, Illinois 61801-2975
`duursma@math.uiuc.edu`