Evaluation Codes from smooth Quadric Surfaces and Twisted Segre Varieties

Alain Couvreur [*] and Iwan Duursma [†]

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 of 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.

MSC: 94B27, 11T71, 14G50, 94B15.
Keywords: Evaluation codes, Algebraic Geometry codes, quadric surfaces, BCH codes, Segre embedding.

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 [3]. Most of the results on the topic concern the evaluation of forms of degree 1 or 2. 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 [2]. 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.

[*] Université Bordeaux I, Institut de Matématiques de Bordeaux

[†] Department of Mathematics, University of Illinois at Urbana-Champaign

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 generalization 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 realization of a large class of BCH codes as evaluation codes and without using a subfield subcode operation.

The paper is organized 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.

1 Prerequisites

1.1 Evaluation codes

Let $X \subset \mathbf{P}^r$ be a smooth projective variety over $\mathbf{F}_q$. Let $\mathcal{F}_r := \mathbf{F}_q[x_0, \ldots, x_r]$ be the graded coordinate ring of $\mathbf{P}^r$ and for all integer s, denote by $\mathcal{F}_r(s)$ its subspace of homogeneous forms of degree 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 $(0 : \ldots : 0 : 1 : p_i : \ldots : p_r)$.

The evaluation code $C_X(s)$ is defined as the image of the evaluation map

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

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 $I_X \subset \mathcal{F}_r$ associated to X, then the above map ev obviously factors as $ev : \mathcal{F}_r(s)/I_X(s) \to \mathbf{F}_q^n$.

The codes $C_X(s)$ with $X = \mathbf{P}^r$ are the projective Reed-Muller codes $PC_s(r, q)$ and their parameters were obtained by Sorensen [10, 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 Quadric surfaces

Over a finite field $\mathbf{F}_q$ there exists two distinct isomorphism classes of smooth quadric surfaces, respectively called *elliptic quadrics* and *hyperbolic quadrics* (see [6] for further details).

1.3.1 Rational parametrization of quadrics

Elliptic and hyperbolic quadrics are both rational. Here is a parametrization of the hyperbolic quadric with equation $x_0x_3 - x_1x_2 = 0$.

$$\left\{ \begin{array}{ccc} \mathbf{P}^2 & \dashrightarrow & \mathbf{P}^3 \\ (x:y:z) & \longmapsto & (z^2 : xz : yz : xy) \end{array} \right. . \tag{1}$$

Let $Q(x,y)$ be an irreducible homogeneous polynomial of degree 2 over $\mathbf{F}_q$, then the following map yields a rational parametrization of the elliptic quadric with equation $x_0x_3 - Q(x_1,x_2) = 0$

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

Remark 1.1. From the above descriptions of these quadrics, one can easily prove that the elliptic quadric is a twist of the hyperbolic one. Let $(x-wy)(x-w^qy)$ be the factorization of Q over $\mathbf{F}_{q^2}$ (with $w \in \mathbf{F}_{q^2} \setminus \mathbf{F}_q$). The $\mathbf{F}_{q^2}$–map $(x_0 : x_1 : x_2 : x_3) \to (x_0 : x_1 - wx_2 : x_1 - w^qx_2 : x_3)$ induces an $\mathbf{F}_{q^2}$–isomorphism between the elliptic and the hyperbolic quadric.

Remark 1.2. The elliptic quadric is unique up to projective equivalence. This entails that, in the above description, if we replace Q by another irreducible degree 2 polynomial, we get another elliptic quadric which is projectively equivalent to the first one.

2 Codes on 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 [4, Chapter 4 §4], [9, Chapter I §5.1] for a definition of the Segre embedding):

$$\phi : \left\{ \begin{array}{ccc} \mathbf{P}^1 \times \mathbf{P}^1 & \to & \mathbf{P}^3 \\ ((u_0 : v_0), (u_1 : v_1)) & \mapsto & (u_0u_1 : u_0v_1 : v_0u_1 : v_0v_1) \end{array} \right. .$$

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 [5, 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. Using 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.

Theorem 2.1 has the following geometric corollary.

Corollary 2.4 (Maximum number of points of a (s,s) curve)**.** *Let X be a curve obtained by the intersection of $\mathcal{H}$ with a hypersurface 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 1. 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 $\mathcal{H}$. □

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 the 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) punctured at two positions yield a BCH code of length q^2-1.

The cyclic structure of the punctured codes can be explained geometrically. Indeed, the automorphism group of $\mathcal{E}$ acts 2-transitively on rational points and the stabilizer of two points contains a linear automorphism permuting cyclically the q^2-1 other points.

3.1 A class of BCH codes

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

This class of codes is studied in [2] and the following result is obtained.

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. [2, Proposition 12] . □

Remark 3.3. Observe that the code $B(s)$ is defined over $\mathbf{F}_q$ and there exists a generator matrix defined over $\mathbf{F}_q$ that generates $B_0(s)$ (with coefficients chosen in $\mathbf{F}_q$) as well as $B(s)$ (with coefficients chosen in $\mathbf{F}_{q^2}$). Thus $B_0(s)$ and $B(s)$ have the same parameters. The condition $0 \leq u, v \leq s$ differs from the condition $0 \leq u + v \leq s$ that is used to describe punctured Reed-Muller codes as cyclic codes.

3.2 Codes on the elliptic quadric

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

The point of the following statements is to show that the code $C_{\mathcal{E}}(s)$ punctured at two positions is the BCH code $B_0(s)$ up to a reordering of the coordinates. Let us choose two points which will correspond to the punctured positions.

Notation 3.4. From now on, we choose an irreducible homogeneous polynomial $Q(x_1, x_2)$ and define $\mathcal{E} \subset \mathbf{P}^3$ by the equation $x_0x_3 - Q(x_1, x_2) = 0$ as in (2). Let P_0 and P_∞ be the points of $\mathbf{P}^3$ with coordinates $(0:0:0:1)$ and $(1:0:0:0)$, respectively. Both points are contained in $\mathcal{E}$. We denote by $C_{\mathcal{E}}^*(s)$ the code $C_{\mathcal{E}}(s)$ punctured at the two positions corresponding to P_0 and P_∞.

The following theorem, proved in §3.2.2 is central in our study.

Theorem 3.5. *For all $s < q$, the code $C_{\mathcal{E}}^*(s)$ defined in Notation 3.4 is permutation equivalent to the code $B_0(s)$ introduced in §3.1.*

3.2.1 The affine parametrization

First, we should notice that P_∞ is the only rational point of $\mathcal{E} \cap \{x_0 = 0\}$. Thus, one can work in the affine chart $\mathcal{U} := \mathcal{E} \cap \{x_0 \neq 0\}$. Using (2), we get the following affine parametrization of $\mathcal{U}$

$$\left\{ \begin{array}{ccc} \mathbf{A}^2 & \to & \mathbf{A}^3 \\ (x,y) & \mapsto & (x,y,Q(x,y)) \end{array} \right. . \tag{3}$$

Remark 3.6. The image of the origin of $\mathbf{A}^2$ by the above map is the point P_0. Thus, there is a one–to–one correspondence between the points of $\mathbf{A}^2(\mathbf{F}_q) \setminus \{(0,0)\}$ and the points of $\mathcal{E}$ supporting the code $C^*_{\mathcal{E}}(s)$.

3.2.2 Equality of codes

First, we state an elementary combinatorial lemma.

Lemma 3.7. *For all nonnegative integer s, the sets $U_s := \{(i+k, j+k) \mid i,j,k \geq 0$ and $i+j+k \leq s\}$ and $V_s := \{(i',j') \mid 0 \leq i',j' \leq s\}$ are equal.*

Proof. The inclusion $U_s \subset V_s$ is obvious. Conversely, let $(i',j') \in V_s$. If $i'+j' \leq s$, then set $k := 0$, else set $k := (i'+j') - s$. Then, for $i := i' - k$ and $j := j' - k$, we get $(i',j') = (i+k, j+k) \in U_s$. □

We can now proceed to the proof of Theorem 3.5.

Proof of Theorem 3.5. Consider the base field extension $C^*_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}$. From Remark 3.3, the subfield subcode of this code over $\mathbf{F}_q$ is $C^*_{\mathcal{E}}(s)$. We will prove that $C^*_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2} = B(s)$, and the theorem then follows from Definition 3.1 and

$$C^*_{\mathcal{E}}(s) = C^*_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}|_{\mathbf{F}_q} = B(s)|_{\mathbf{F}_q} = B_0(s).$$

We use the affine point of view described in §3.2.1 and denote by (x,y,z) a system of coordinates of $\mathbf{A}^3$. The code $C^*_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}$ is obtained by evaluating at all the $\mathbf{F}_q$–rational points of $\mathcal{U} \setminus \{P_0\}$ the functions of the space $\mathbf{F}_{q^2}[x,y,z]_{\leq s}$ of polynomials with total degree lower than or equal to s.

Let $w \in \mathbf{F}_{q^2}$ be the element of $\mathbf{F}_{q^2} \setminus \mathbf{F}_q$ such that $Q(x,y) = (x+wy)(x+w^q y)$ over $\mathbf{F}_{q^2}$ (without loss of generality, one can assume that the coefficient of x^2 in Q is 1). Consider the family of polynomials

$$f_{i,j,k} := (x - wy)^i (x - w^q y)^j z^k, \quad i+j+k \leq s.$$

The polynomials $f_{i,j,k}$ yield an $\mathbf{F}_{q^2}$–basis of $\mathbf{F}_{q^2}[x,y,z]_{\leq s}$. Pulling back this basis by the map described in (3), we get the family of polynomials

$$f^\star_{i,j,k} := (x+wy)^i (x+w^q y)^j Q(x,y)^k = (x+wy)^{i+k} (x+w^q y)^{j+k},$$

for $i+j+k \leq s$. Therefore, using the map (3) together with Remark 3.6, we see that $C_{\mathcal{E}}(s)^* \otimes \mathbf{F}_{q^2}$ is generated over $\mathbf{F}_{q^2}$ by the words

$$(f^\star_{i,j,k}(x,y) \mid (x,y) \in \mathbf{F}_q^2 \setminus \{0,0\}), \quad \text{for } i+j+k \leq s.$$

Finally, for $\zeta \in \mathbf{F}_{q^2}$, there exist unique $a, b \in \mathbf{F}_q$ such that $\zeta = a + wb$, and

$$f^{\star}_{i,j,k}(a,b) = \zeta^{i+k}\bar{\zeta}^{(j+k)},$$

where $\bar{\zeta}$ denotes the conjugate of ζ under the Frobenius action. That is $\bar{\zeta} := \zeta^q$. We conclude that $C^*_{\mathcal{E}}(s) \otimes \mathbf{F}_{q^2}$ is generated over $\mathbf{F}_{q^2}$ by the words

$$(\zeta^{i+k}\zeta^{q(j+k)} \mid \zeta \in \mathbf{F}^{\times}_{q^2}), \quad \text{for } i+j+k \leq s.$$

Using Lemma 3.7, the code is generated by the words

$$(\zeta^{i'+qj'} \mid \zeta \in \mathbf{F}^{\times}_{q^2}), \quad \text{for } i', j' \leq s,$$

and hence this code is nothing but the code $B(s)$. This yields the result. □

3.3 The parameters of the codes on the elliptic quadric

As a conclusion we have the following result.

Theorem 3.8. *For all $s < q-1$, the code $C_{\mathcal{E}}(s)$ has parameters $[q^2+1, (s+1)^2, q^2+1-s(q+1)]$*

Proof. From Theorem 3.5 and Proposition 3.2, this code punctured at two positions has parameters $[q^2-1, (s+1)^2, q^2-1-s(q+1)]$. Thus, $C_{\mathcal{E}}(s)$ has dimension at least $(s+1)^2$ and minimum distance between $q^2-1-s(q+1)$ and $q^2+1-s(q+1)$.

Let c be a minimum weight codeword of $C_{\mathcal{E}}(s)$. By the previous assertion, the weight of c satisfies $w(c) \geq q^2-1-s(q+1)$. Moreover, since s is assumed to be $< q-1$, then $w(c) \geq q+1 \geq 3$. This word is obtained by the evaluation of $f \in \mathcal{F}_3(s)$. Since the automorphism group of $\mathcal{E}$ acts 2–transitively, one can assume that f does not vanish on P_0 and P_∞ (see Notation 3.4). Therefore, if $c^* \in C_{\mathcal{E}}(s)^*$ denotes the punctured codeword c, then $w(c^*) = w(c) - 2$ and hence $w(c) \geq q^2+1-s(q+1)$. Consequently, the code has minimum distance $q^2+1-s(q+1)$.

Finally, let us prove that the dimension is $(s+1)^2$. Since the minimum distance of $C_{\mathcal{E}}(s)$ is > 2, then no codeword can be sent to zero by puncturing. Thus, the puncturing map $C_{\mathcal{E}}(s) \to C_{\mathcal{E}}(s)^*$ is an isomorphism and hence, both codes have the same dimension □

Remark 3.9. As in Remark 2.3, one can prove using the structure of the Picard group of $\mathcal{E}$ that any evaluation code on this surface is equivalent to $C_{\mathcal{E}}(s)$ for some s.

Theorem 3.8 has a geometric corollary.

Corollary 3.10. *Let $s < q-1$. Let $X \subset \mathcal{E}$ be a curve obtained by the intersection of $\mathcal{E}$ with a hypersurface of degree s which does not contain $\mathcal{E}$. Then,*

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

Proof. It is a straightforward consequence of Theorem 3.8 □

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. Both approaches generalize and in this section we will describe evaluation codes defined on the image $X \subset \mathbf{P}^r$ of Segre embedding $\phi : \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \longrightarrow \mathbf{P}^{2^d-1}$ of d copies of $\mathbf{P}^1$.

It is well–known that the homogeneous ideal $I_X \subset \mathcal{F}_r = \mathbf{F}_q[x_0, \ldots, x_r]$ for X 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 [8]).

The case of the embedding of $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$ has a rational parametrization

$$\left\{ \begin{array}{ccc} \mathbf{P}^3 & \dashrightarrow & \mathbf{P}^7 \\ (x:y:z:t) & \longmapsto & (t^3 : t^2x : t^2y : t^2z : txy : tyz : tzx : xyz) \end{array} \right. . \tag{4}$$

The image is the intersection in $\mathbf{P}^7$ of nine quadrics that 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 $x \mapsto y \mapsto z \mapsto x$. The full resolution, given in [7], is

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

4.1 The non-twisted case

Without proof, which is similar to the case of smooth quadrics in $\mathbf{P}^3$ and which will be available in an extended version, we give the parameters of evaluation codes on the embedding $X = \mathbf{P}^1 \times \cdots \times \mathbf{P}^1 \subset \mathbf{P}^{2^d-1}$ and on twists of X over $\mathbf{F}_{q^d}$.

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.*

4.2 The twisted case

Definition 4.2. Let d be a positive integer and $\alpha_1, \ldots, \alpha_d$ be an $\mathbf{F}_q$–basis of $\mathbf{F}_{q^d}$. The twist $\mathcal{E}$ over $\mathbf{F}_{q^2}$ is obtained from $\mathcal{H}$ by the change of variables

$$\left\{ \begin{array}{lcl} x'_0 & := & x_0 \\ x'_j & := & \alpha_1^{q^{j-1}} x_1 + \cdots + \alpha_d^{q^{j-1}} x_d, \quad \text{for } j \in \{1, \ldots, d\} \end{array} \right. .$$

Theorem 4.3. *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 twice punctured code $C^*_{\mathcal{E}}(s)$ is a BCH code.*

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

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

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

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

[6] 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.

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

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

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

[10] 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