# Reed-Muller Codes Associated to Projective Algebraic Varieties

Yves AUBRY

Equipe CNRS "Arithmétique et Théorie de l'Information"

C.I.R.M. Luminy Case 916 - 13288 Marseille Cedex 9 - France.

## Abstract

The classical generalized Reed-Muller codes introduced by Kasami, Lin and Peterson [5], and studied also by Delsarte, Goethals and Mac Williams [2], are defined over the affine space $\mathbf{A}^n(\mathbf{F}_q)$ over the finite field $\mathbf{F}_q$ with q elements. Moreover Lachaud [6], following Manin and Vladut [7], has considered projective Reed-Muller codes, i.e. defined over the projective space $\mathbf{P}^n(\mathbf{F}_q)$.
In this paper, the evaluation of the forms with coefficients in the finite field $\mathbf{F}_q$ is made on the points of a projective algebraic variety V over the projective space $\mathbf{P}^n(\mathbf{F}_q)$. Firstly, we consider the case where V is a quadric hypersurface, singular or not, Parabolic, Hyperbolic or Elliptic. Some results about the number of points in a (possibly degenerate) quadric and in the hyperplane sections are given, and also is given an upper bound of the number of points in the intersection of two quadrics.

In application of these results, we obtain Reed-Muller codes of order 1 associated to quadrics with three weights and we give their parameters, as well as Reed-Muller codes of order 2 with their parameters.

Secondly, we take V as a hypersurface, which is the union of hyperplanes containing a linear variety of codimension 2 (these hypersurfaces reach the Serre bound). If V is of degree h, we give parameters of Reed-Muller codes of order $d < h$, associated to V.

## 1. Construction of the Projective Reed-Muller codes

We denote by $\mathbf{P}^n(\mathbf{F}_q)$ the projective space of dimension n over the finite field $\mathbf{F}_q$ with q elements, q a power of a prime p. The number of (rational) points (over $\mathbf{F}_q$) of $\mathbf{P}^n(\mathbf{F}_q)$ is :

$$\pi_n = |\, \mathbf{P}^n(\mathbf{F}_q) \,| = q^n + q^{n-1} + \ldots + q + 1 = \frac{q^{n+1} - 1}{q - 1} .$$

Let $W_i$ be the set of points with homogeneous coordinates $(x_0 : x_1 : ... : x_n) \in \mathbf{P}^n(\mathbf{F}_q)$ such that

$$x_0 = x_1 = ... = x_{i-1} = 0 \text{ and } x_i \neq 0.$$

The family $\{ W_i \}_{0 \leq i \leq n}$ is clearly a partition of $\mathbf{P}^n(\mathbf{F}_q)$.

Let $\mathbf{F}_q[X_0, X_1, ..., X_n]_d^0$ be the vector space of homogeneous polynomials of degree d with (n+1) variables and with coefficients in $\mathbf{F}_q$. Let $\mathbf{V}$ be a projective algebraic variety of $\mathbf{P}^n(\mathbf{F}_q)$ and let $|\mathbf{V}|$ denotes the number of theirs rational points over $\mathbf{F}_q$. Following G. Lachaud ([6]), we define the *projective Reed-Muller code* $\mathcal{R}(d,\mathbf{V})$ of order d associated to the variety $\mathbf{V}$ as the image of the linear map

$$\mathbf{c} : \mathbf{F}_q[X_0, X_1, ..., X_n]_d^0 \rightarrow \mathbf{F}_q^{|V|}$$

defined by $\mathbf{c}(P) = ( c_x(P) )_{x \in \mathbf{V}}$, where

$$c_x(P) = \frac{P(x_0, ..., x_n)}{x_i^d} \text{ if } x = (x_0 : ... : x_n) \in W_i \ .$$

G. Lachaud has considered in [6] the case where $\mathbf{V} = \mathbf{P}^n(\mathbf{F}_q)$, with $d \leq q$.Moreover, A.B. Sorensen has considered in [12] the case where $\mathbf{V}$ is equal to $\mathbf{P}^n(\mathbf{F}_q)$ too, but with a weaker hypothesis on d.

Now we are going, firstly, to study the case where $\mathbf{V}$ is a quadric, degenerate or not, but before we have to establish results on quadrics and this is the subject of the following paragraph.

## 2. Results on quadrics

In what follows the characteristic of the field $\mathbf{F}_q$ is supposed to be arbitrary (the results hold in characteristic 2 as well as in characteristic different of 2).

### 2.1. The quadrics in $\mathbf{P}^n(\mathbf{F}_q)$.

In this paragraph, we recall some properties of quadrics in the projective space $\mathbf{P}^n(\mathbf{F}_q)$. J.F. Primrose has given in [8] the number of points in a nondegenerate quadric (see below the definition of the rank of a quadric), and D.K. Ray-Chaudhuri [9] gave more general results (which with, in a particular case, we recover those of Primrose's). We are going here to follow the notations of J.W.P. Hirschfeld in [4].

A quadric Q of $\mathbf{P}^n(\mathbf{F}_q)$ is the set of zeros in $\mathbf{P}^n(\mathbf{F}_q)$ of a quadratic form

$$F \in \mathbf{F}_q[X_0, X_1, ..., X_n]_2^0,$$

that is of an homogeneous polynomial of degree 2. We set $Q = Z_{\mathbf{P}^n}(F)$ or simply Z(F) if no confusion is possible. The quadric Q is said to be *degenerate* if there exists a linear change of coordinates with which we can write the form F with a fewer number of variables. More precisely, if T is an invertible linear transformation defined over $\mathbf{P}^n(\mathbf{F}_q)$, denote by $F_T(X)$ the form F(TX). Let i(F) be the number of indeterminates appearing explicitly in F. The rank r(F) of F (and by abuse of language, of the quadric Q), is defined by :

$$r(F) = \min_T i(F_T)$$

where T ranges over all the invertible transformations defined over $\mathbf{F}_q$. A form F (and by abuse the quadric Q) is said to be *degenerate* if

$$r(F) < n + 1.$$

Otherwise, the form and the quadric are *nondegenerate*.
Let us remark that a quadric is degenerate if and only if it is singular (see [4]).

We recall after J.W.P. Hirschfeld (see [4]) that in $\mathbf{P}^n(\mathbf{F}_q)$, the number of different types of nondegenerate quadrics Q is 1 or 2 as n is even or odd, and they are respectively called *Parabolic* ($\mathcal{P}$), and *Hyperbolic* ($\mathcal{H}$) or *Elliptic* ($\mathcal{E}$).
The maximum dimension g(Q) of linear subspaces lying on the nondegenerate quadric Q is called the *projective index* of Q. The projective index has the following values (see [4]) :

$$g(\mathcal{P}) = \frac{n-2}{2} \quad , \quad g(\mathcal{H}) = \frac{n-1}{2} \quad , \quad g(\mathcal{E}) = \frac{n-3}{2} \quad .$$

The character $\omega(Q)$ of a nondegenerate quadric Q of $\mathbf{P}^n(\mathbf{F}_q)$ is defined by :

$$\omega(Q) = 2g(Q) - n + 3.$$

Consequently, we have :

$$\omega(\mathcal{P}) = 1 \quad , \quad \omega(\mathcal{H}) = 2 \quad , \quad \omega(\mathcal{E}) = 0 \quad .$$

Then, we have the following proposition (for a proof see [4]) :

**Proposition 1 :** The number of points of a nondegenerate quadric Q of $\mathbf{P}^n(\mathbf{F}_q)$ is :

$$|Q| = \pi_{n-1} + (\omega(Q) - 1)\, q^{(n-1)/2} .$$

We want now to evaluate the number of points of a degenerate quadric Q = Z(F) of $\mathbf{P}^n(\mathbf{F}_q)$ of rank r (called a "cone" of rank r).
We have the following decomposition in disjoint union (an analogous decomposition is given by R.A. Games in [3]) :

$$Q = V_{n-r} \cup Q^*_{r-1}.$$

We have set

$$V_{n-r} = \{(0 : 0 : \ldots : 0 : y_r : \ldots : y_n) \in \mathbf{P}^n(\mathbf{F}_q)\} \cong \mathbf{P}^{n-r}(\mathbf{F}_q),$$

if we suppose that the r variables appearing in the quadratic form F are $X_0, X_1, \ldots, X_{r-1}$. The set $V_{n-r}$ is called the vertex of Q, and is the set of singular points of Q. We note also

$$Q^*_{r-1} = \{(x_0 : \ldots : x_{r-1} : y_r : \ldots : y_n) \in \mathbf{P}^n(\mathbf{F}_q) \mid F(x_0, \ldots, y_n) = 0 \text{ and the } x_i \text{ are not all zero}\}.$$

Let $Q_{r-1}$ be the nondegenerate quadric of $\mathbf{P}^{r-1}(\mathbf{F}_q)$ associated to Q, i.e. defined by

$$Q_{r-1} = Z_{\mathbf{P}^{r-1}}(F_{r-1})$$

or more precisely,

$$Q_{r-1} = \{ (x_0 : \dots : x_{r-1}) \in \mathbf{P}^{r-1}(\mathbf{F}_q) \mid F_{r-1}(x_0, \dots, x_{r-1}) = 0 \},$$

where $F_{r-1}(X_0, \dots, X_{r-1}) = F(X_0, \dots, X_n)$. The (degenerate) quadric Q will abusively be said to be parabolic, hyperbolic or elliptic according to the type of its associated nondegenerate quadric $Q_{r-1}$. Its character $\omega(Q)$ is by definition the character $\omega(Q_{r-1})$ of $Q_{r-1}$.
Then, we have the following result which can be found in R.A. Games [3] :

**Theorem 1 :** The number of points of a quadric Q of $\mathbf{P}^n(\mathbf{F}_q)$ of rank r is :

$$| Q | = \pi_{n-1} + (\omega(Q) - 1)\, q^{(2n-r)/2}$$

and we have $\omega(Q) = 1$ if r is odd, and $\omega(Q) = 0$ or $\omega(Q) = 2$ if r is even.

In particular, a quadric of odd rank is necessarily parabolic, and a quadric of even rank is hyperbolic or elliptic.

**Corollary :** Let Q be a quadric of $\mathbf{P}^n(\mathbf{F}_q)$, with $n \geq 2$. We have :

$$\pi_{n-2} \leq | Q | \leq \pi_{n-1} + q^{n-1},$$

and the bounds are reached.

Observe that the lower bound is the Warning bound and that the upper bound reaches the following Serre bound, conjectured by Tsfasman, which says that (see [11]) if $F \in \mathbf{F}_q[X_0,\dots,X_n]_d^0$ is a nonzero form of degree $d \leq q$, with $n \geq 2$, then the number N of zeros of F in $\mathbf{F}_q^n$ is such that :

$$N \leq d\, q^{n-1} - (d-1)\, q^{n-2}.$$

## 2.2. Hyperplane sections of quadrics.

This paragraph deals with the number of points in the intersection of a quadric and a hyperplane. When the quadric is nondegenerate, the result is known (see for example [13]). R.A. Games has given the result when the quadric has the size of a hyperplane, provided the quadric itself is not a hyperplane (see [3]). Furthermore, I.M. Chakravarti in [1] has solved the case when the quadric is 1-degenerate, that is a quadric of rank n in $\mathbf{P}^n(\mathbf{F}_q)$.
We are going, here, to consider the general case, i.e. quadrics in $\mathbf{P}^n(\mathbf{F}_q)$ of any rank.

We begin by the known nondegenerate case. If Q is a nondegenerate quadric of $\mathbf{P}^n(\mathbf{F}_q)$ (i.e. of rank $r = n + 1$) and if H is a hyperplane of $\mathbf{P}^n(\mathbf{F}_q)$, with $n > 1$, then $Q \cap H$ can be seen as a quadric in a space of dimension $n - 1$. We know (see for example [8]) that the rank of $Q \cap H$ is $r - 1$ or $r - 2$. Then, either $Q \cap H$ is nondegenerate (in $\mathbf{P}^{n-1}(\mathbf{F}_q)$), or $Q \cap H$ is of rank $r - 2 = n - 1$ (whence degenerate in $\mathbf{P}^{n-1}(\mathbf{F}_q)$) ; one says in this last case that H is *tangent* to Q.

Now we have to know what is the value of $\omega(Q \cap H)$, i.e. what happens to the type of the quadric. If the hyperplane H is not tangent to Q, it is obvious that $Q \cap H$ becomes parabolic if Q is hyperbolic or elliptic (indeed r(Q) is necessarily even, and if H is not tangent we have $r(Q \cap H) = r(Q) - 1$ hence odd, then $Q \cap H$ is parabolic) ; and $Q \cap H$ becomes hyperbolic or elliptic if Q is parabolic (same reason rest on the parity of the ranks).
Now if the hyperplane H is tangent to Q, we have the following proposition (see [13]) :

**Proposition 2** : The quadric $Q \cap H$ is of the same type as the nondegenerate quadric Q if the hyperplane H is tangent to Q.

Then, we can give the result about the hyperplane sections of a quadric of any rank :

**Theorem 2** : Let Q be a quadric of $\mathbf{P}^n(\mathbf{F}_q)$ of rank r whose decomposition is

$$Q = V_{n-r} \cup Q^*_{r-1}$$

and let H be a hyperplane of $\mathbf{P}^n(\mathbf{F}_q)$. Then :

a) If $H \supset V_{n-r}$ then

$$|Q \cap H| = \pi_{n-2} + (\omega(Q_{r-1} \cap H_*) - 1)\, q^{(2n-r-1)/2}$$

if $H_*$ is not tangent to $Q_{r-1}$, and

$$|Q \cap H| = \pi_{n-2} + (\omega(Q) - 1)\, q^{(2n-r)/2}$$

if $H_*$ is tangent to $Q_{r-1}$, where $H_*$ is the hyperplane of $\mathbf{P}^{r-1}(\mathbf{F}_q)$ defined by

$$H_* = Z_{\mathbf{P}^{r-1}}(h)$$

where h is the linear form in $\mathbf{F}_q[X_0,\ldots,X_{r-1}]_1^0$ defining H ; moreover $\omega(Q_{r-1} \cap H_*)$ is equal to 1 if Q is hyperbolic or elliptic, and equal to 0 or 2 if Q is parabolic.

b) If $H \not\supset V_{n-r}$ then

$$|Q \cap H| = \pi_{n-2} + (\omega(Q) - 1)\, q^{(2n-r-2)/2}\,.$$

*Proof* : We suppose that the r variables appearing in the quadratic form F defining Q are $X_0, X_1, \ldots, X_{r-1}$ .
If we set $H_i$ the hyperplane whose equation is $X_i = 0$, we have

$$V_{n-r} = H_0 \cap H_1 \cap \ldots \cap H_{r-1}\,.$$

But

$$Q \cap H = (V_{n-r} \cup Q^*_{r-1}) \cap H = (V_{n-r} \cap H) \cup (Q^*_{r-1} \cap H),$$

Thus

$$|Q \cap H| = |V_{n-r} \cap H| + |Q^*_{r-1} \cap H| - |V_{n-r} \cap Q^*_{r-1} \cap H|\,;$$

but $V_{n-r} \cap Q^*_{r-1} = \varnothing$ , thus :

$$|Q \cap H| = |V_{n-r} \cap H| + |Q^*_{r-1} \cap H|.$$

1°) Suppose that $H \supset V_{n-r}$.

Then, we have : $| V_{n-r} \cap H | = | V_{n-r} | = | \mathbf{P}^{n-r}(\mathbf{F}_q) | = \pi_{n-r}$.

Furthermore, the linear form h defining H is such that $h \in \mathbf{F}_q[X_0,...,X_{r-1}]_1^0$. Indeed, if

$$h = \sum_{i=0}^{n} a_i X_i ,$$

we have for all $i \geq r$, $P_i = (0 : ... : 0 : 1 : 0 : ... : 0)$ where the 1 is at the $i^{th}$ - coordinate, $P_i \in V_{n-r}$ and $H \supset V_{n-r}$ thus $h(P_i) = 0$. But $h(P_i) = a_i$, thus $a_i = 0$ for all $i \geq r$. Hence,

$$| Q^*_{r-1} \cap H | = q^{n-r+1} | Q_{r-1} \cap H_* |.$$

The quadric $Q_{r-1} \cap H_*$ of $\mathbf{P}^{r-2}(\mathbf{F}_q)$ is degenerate or not, according as $H_*$ is tangent or not to $Q_{r-1}$. Now :

— If $H_*$ is not tangent to $Q_{r-1}$, then by proposition 1, (since $Q_{r-1} \cap H_*$ is nondegenerate in $\mathbf{P}^{r-2}(\mathbf{F}_q)$ ), we have :

$$| Q_{r-1} \cap H_* | = \pi_{r-3} + (\omega(Q_{r-1} \cap H_*) - 1)\, q^{(r-3)/2}.$$

Thus

$$| Q \cap H | = \pi_{n-r} + q^{n-r+1} | Q_{r-1} \cap H_* | = \pi_{n-2} + (\omega(Q_{r-1} \cap H_*) - 1)\, q^{(2n-r-1)/2} .$$

— If $H_*$ is tangent to $Q_{r-1}$, then by theorem 1, we have :

$$| Q_{r-1} \cap H_* | = \pi_{r-3} + (\omega(Q_{r-1} \cap H_*) - 1)\, q^{(r-2)/2},$$

but by proposition 2 we know that $\omega(Q_{r-1} \cap H_*) = \omega(Q_{r-1})$,which is equal to $\omega(Q)$ by definition. Finally,

$$\begin{aligned} | Q \cap H | &= \pi_{n-r} + q^{n-r+1} ( \pi_{r-3} + (\omega(Q) - 1)\, q^{(r-2)/2} ) \\ &= \pi_{n-2} + (\omega(Q) - 1)\, q^{(2n-r)/2} . \end{aligned}$$

2°) Suppose now that H not contains $V_{n-r}$.

We have $V_{n-r} \cap H = H_0 \cap H_1 \cap ... \cap H_{r-1} \cap H$, thus

$$| V_{n-r} \cap H | = | \mathbf{P}^{n-r-1}(\mathbf{F}_q) | = \pi_{n-r-1} .$$

If $h = \sum_{i=0}^{n} a_i X_i$ is the linear form defining H, there exist necessarily one j, $r \leq j \leq n$, such that $a_j \neq 0$. Thus

$$\begin{aligned} Q^*_{r-1} \cap H = \{ & (x_0 : ... : x_{r-1} : y_r : ... : y_{j-1} : t : y_{j+1} : ... : y_n) \in \mathbf{P}^n(\mathbf{F}_q) \\ & \text{with } Q_{r-1}(x_0,...,x_{r-1}) = 0 \text{ and the } x_i \text{ are not all zero } \}, \end{aligned}$$

where t is such that

$$a_j t = - a_0 x_0 - ... - a_{r-1} x_{r-1} - a_r y_r - ... - a_{j-1} y_{j-1} - a_{j+1} y_{j+1} - ... - a_n y_n .$$

Thus

$$| Q^*_{r-1} \cap H | = q^{(n-r+1)-1} | Q_{r-1} |$$

with $Q_{r-1}$ a nondegenerate quadric of $\mathbf{P}^{r-1}(\mathbf{F}_q)$, then :

$$| Q^*_{r-1} \cap H | = q^{n-r} ( \pi_{r-2} + (\omega(Q_{r-1}) - 1)\, q^{(r-2)/2} )$$

and finally :

$$| Q \cap H | = \pi_{n-r-1} + q^{n-r} ( \pi_{r-2} + (\omega(Q_{r-1}) - 1)\, q^{(r-2)/2} )$$
$$= \pi_{n-2} + (\omega(Q) - 1)\, q^{(2n-r-2)/2},$$

which concludes the proof. ♦

## 2.3. Intersection of two quadrics in $\mathbf{P}^n(\mathbf{F}_q)$.

The subject matter of this paragraph is to estimate the number of points in the intersection of two quadrics in $\mathbf{P}^n(\mathbf{F}_q)$ with $n > 1$ . We give an exact value of this number in a particular case, and an upper bound in the general case (Theorem 3), inspired by an another upper bound of W.M. Schmidt ([10] p.152). We need first a lemma :

**Lemma** : If $Q_1$ and $Q_2$ are two distinct quadrics in $\mathbf{P}^n(\mathbf{F}_q)$, then :

$$| Q_1 \cap Q_2 | \leq \pi_{n-1} + q^{n-2}.$$

*Proof* : By theorem 1, $| Q_1 | = \pi_{n-1} + (\omega(Q_1) - 1)\, q^{(2n-r)/2}$ if r is the rank of $Q_1$. Thus :

— if $r \geq 4$, we have $\frac{2n-r}{2} \leq n-2$ and then $| Q_1 | \leq \pi_{n-1} + q^{n-2}$ , hence a fortiori

$$| Q_1 \cap Q_2 | \leq \pi_{n-1} + q^{n-2}.$$

— if $r = 3$ or $r = 1$ then $Q_1$ is parabolic and

$$| Q_1 \cap Q_2 | \leq | Q_1 | = \pi_{n-1} < \pi_{n-1} + q^{n-2}.$$

— if $r = 2$ : either $Q_1$ is elliptic, and then $| Q_1 | = \pi_{n-1} - q^{n-1}$ and the result holds ; or $Q_1$ is hyperbolic, and then $Q_1$ is the union of two distinct hyperplanes. We can suppose that the quadric $Q_2$ is also hyperbolic of rank 2, otherwise the same reasoning which we have made to $Q_1$ must hold for $Q_2$.

We set $Q_1 = H_0 \cup H_1$ and $Q_2 = H_2 \cup H_t$ , and without loss of generality, we can take for $H_i$ the hyperplane $X_i = 0$. Since, by hypothesis, the quadrics $Q_1$ and $Q_2$ are distincts, two cases can appear :

1°) The four hyperplanes are distincts, i.e. t is different of 0 and 1. We obtain, simply in "counting" the points :

$$| Q_1 \cap Q_2 | = \pi_{n-4} + 4\, q^{n-2} \leq \pi_{n-1} + q^{n-2}$$

(the preceding inequality is equivalent to $(q-1)^2 \geq 0$ ).

2°) $Q_1$ and $Q_2$ have a common hyperplane, i.e. $t = 0$ or $t = 1$. Suppose that $t = 0$. Then, we have :

$$Q_1 \cap Q_2 = \{ (0 : x_1 : \ldots : x_n) \in \mathbf{P}^n(\mathbf{F}_q) \} \cup \{ (1 : 0 : 0 : x_3 : \ldots : x_n) \in \mathbf{P}^n(\mathbf{F}_q) \},$$

where the union is disjoint. Hence :

$| Q_1 \cap Q_2 | = \pi_{n-1} + q^{n-2}$ , and the upper bound of this lemma is reached in this case. ♦

**Theorem 3** : Let $F_1(X_0,...,X_n)$ and $F_2(X_0,...,X_n)$ be two non zero quadratic forms with coefficients in $\mathbf{F}_q$, and let $Q_1$ and $Q_2$ respectively the two associated quadrics of $\mathbf{P}^n(\mathbf{F}_q)$. Three cases can appear :

1°) the forms $F_1$ and $F_2$ are proportional (i.e there exists $\lambda \in \mathbf{F}_q^*$ such that $F_1 = \lambda F_2$ ) and then :

$$| Q_1 \cap Q_2 | = | Q_1 | = | Q_2 | .$$

2°) $F_1$ and $F_2$ have a common factor of degree 1, and then :

$$| Q_1 \cap Q_2 | = \pi_{n-1} + q^{n-2} .$$

3°) $F_1$ and $F_2$ have no common factor (no constant), and then :

$$| Q_1 \cap Q_2 | \leq \pi_{n-2} + \frac{7\, q^{n-1}}{q-1} - \frac{6\, q^{n-2}}{q-1}$$

(for $q \geq 7$ this upper bound is indeed better than the lemma).

*Proof* : 1°) Trivial.

2°) We are necessarily in the case where $Q_1$ and $Q_2$ are the union of two hyperplanes with one in common ; it is proved in the lemma.

3°) Let $F_1$ and $F_2$ be two quadratic forms without nonconstant common factor.

The result is obvious if $q \leq 4$. Indeed, by the lemma, we have :

$$| Q_1 \cap Q_2 | \leq \pi_{n-1} + q^{n-2}$$

and furthermore,

$\pi_{n-1} + q^{n-2} \leq \pi_{n-2} + \frac{7\, q^{n-1}}{q-1} - \frac{6\, q^{n-2}}{q-1}$ is equivalent to $q \leq 5$.

Suppose now that $q > 4$.

We set, for i equal 1 and 2 :

$$F'_i(X_0,...,X_n) = F_i(X_0 , X_1+c_1X_0 , X_2+c_2X_0 , ... , X_n+c_nX_0)$$
$$= P_i(c_1,c_2,...,c_n)\, X_0^2 + ... .$$

The polynomials $P_1$ and $P_2$ are not the zero polynomial (otherwise $F_1$ and $F_2$ would be too), and are not also identically zero, since they have degree at most 2, and $q > 4$ implies that $F_1$ and $F_2$ have at most $2q^{n-1} < q^n$ zeros in $\mathbf{F}_q^n$ (because a polynomial of degree d in $\mathbf{F}_q[X_1,...,X_n]$ have at most $dq^{n-1}$ zeros in $\mathbf{F}_q^n$ , see for example [10]).

Moreover, the total number of zeros of $P_1$ added to those of $P_2$ is then at most

$$4\, q^{n-1}$$

which is $< q^n$ since $q > 4$ .

Thus it is possible to choose $(c_1,...,c_n) \in \mathbf{F}_q^n$ such that

$$P_1(c_1,...,c_n) \neq 0 \text{ and } P_2(c_1,...,c_n) \neq 0.$$

Thus, after a nonsingular linear transformation and after divided by $P_1(c_1,...,c_n)$ and $P_2(c_1,...,c_n)$ respectively, we may suppose without loss of generality that :

$$F_1(X_0,...,X_n) = X_0^2 + X_0\, g_1(X_1,...,X_n) + g_2(X_1,...,X_n) \text{ and}$$

$$F_2(X_0,...,X_n) = X_0^2 + X_0\, h_1(X_1,...,X_n) + h_2(X_1,...,X_n)$$

where $g_1,h_1 \in \mathbf{F}_q[X_1,...,X_n]_1^0$ and $g_2,h_2 \in \mathbf{F}_q[X_1,...,X_n]_2^0$.

If we look at now the polynomials $F_1$ and $F_2$ as polynomials in $X_0$, their resultant is a homogeneous polynomial $R(X_1,...,X_n)$ of degree 4. By the well known properties of the resultant, we can say that for any common zero (in $\mathbf{F}_q^{n+1}$) $(x_0,x_1,...,x_n)$ of $F_1(X_0,...,X_n)$ and $F_2(X_0,...,X_n)$, we have $R(x_1,...,x_n) = 0$.
If we apply the Serre bound (see § 2.1) to the resultant R, we obtain that

$$\text{the number of zeros in } \mathbf{F}_q^n \text{ of } R(X_1,...,X_n) \text{ is } \leq 4\,q^{n-1} - 3\,q^{n-2}.$$

Moreover, for such n-uple , the number of possibilities for $x_0$ is at most 2, and the forms $F_1$ and $F_2$ are of degree 2, thus the total number of common zeros $(x_0,...,x_n)$ of $F_1$ and $F_2$ in $\mathbf{F}_q^{n+1}$ is $\leq 8\,q^{n-1} - 6\,q^{n-2}$.
And by the following usual equality :

$$N_A(F) = 1 + (q-1)\,N_P(F)$$

where $N_A(F)$ represent the number of zeros in $\mathbf{A}^{n+1}(\mathbf{F}_q) = \mathbf{F}_q^{n+1}$ of F and $N_P(F)$ the number of zeros in $\mathbf{P}^n(\mathbf{F}_q)$ of F, we deduce :

$$|\,Q_1 \cap Q_2\,| \leq \frac{8\,q^{n-1} - 6\,q^{n-2} - 1}{q-1}$$

$$= \pi_{n-2} + 6\,q^{n-2} + \frac{q^{n-1}}{q-1} = \pi_{n-2} + \frac{7\,q^{n-1}}{q-1} - \frac{6\,q^{n-2}}{q-1}\,.\blacklozenge$$

## 3. Projective Reed-Muller codes of order 1 associated to a quadric

Let Q be a quadric in $\mathbf{P}^n(\mathbf{F}_q)$ of rank r, decomposing in disjoint union of its vertex $V_{n-r}$ and of $Q^*_{r-1}$, where $Q_{r-1}$ is the nondegenerate associated quadric of $\mathbf{P}^{r-1}(\mathbf{F}_q)$. We will apply the results of § 2.2 to determine the parameters of the projective Reed-Muller codes of order 1 associated to Q. Since these parameters vary according to the type of the quadric Q, we have to distinguish three cases.

**Theorem 4** (parabolic case) : Let Q be a parabolic quadric of $\mathbf{P}^n(\mathbf{F}_q)$ of rank $r \neq 1$. Then the projective Reed-Muller code of order 1 associated to Q is a code with three weights :

$$w_1 = q^{n-1} - q^{(2n-r-1)/2},\ w_2 = q^{n-1} + q^{(2n-r-1)/2},\ w_3 = q^{n-1}$$

with the following parameters :

$$\text{length} = \pi_{n-1},\ \text{dimension} = n+1,\ \text{distance} = q^{n-1} - q^{(2n-r-1)/2}\,.$$

**Theorem 5** (hyperbolic case) : Let Q be an hyperbolic quadric of $\mathbf{P}^n(\mathbf{F}_q)$ of rank r. Then the projective Reed-Muller code of order 1 associated to Q is a code with three weights :

$$w_1 = q^{n-1} + q^{(2n-r)/2},\ w_2 = q^{n-1},\ w_3 = q^{n-1} + q^{(2n-r)/2} - q^{(2n-r-2)/2}$$

with the following parameters :

$$\text{length} = \pi_{n-1} + q^{(2n-r)/2},\ \text{dimension} = n+1,\ \text{distance} = q^{n-1}\,.$$

**Theorem 6** (elliptic case) : Let Q be an elliptic quadric of $\mathbf{P}^n(\mathbf{F}_q)$ of rank $r > 2$. Then the projective Reed-Muller code of order 1 associated to Q is a code with three weights :

$$w_1 = q^{n-1} - q^{(2n-r)/2}\,,\ w_2 = q^{n-1}\,,\ w_3 = q^{n-1} - q^{(2n-r)/2} + q^{(2n-r-2)/2}$$

with the following parameters :

$$\text{length} = \pi_{n-1} - q^{(2n-r)/2},\ \text{dimension} = n+1,\ \text{distance} = q^{n-1} - q^{(2n-r)/2}\,.$$

Let us remark that we recover the results of J. Wolfmann as a particular case of these results (see [13]), indeed he had considered the case of nondegenerate quadrics : his results correspond to the case where the rank $r = n+1$. Note that, here, the case $H \not\supset V_{n-r}$ is excluded, and then we find only two weights for the hyperbolic and elliptic quadrics, but still three weights for the parabolic one. We recover also the results of I.M. Chakravarti (see [1]) : it corresponds to the case where the rank $r = n$.

*Proof* : The lengths of the respective codes are equal to the number of points of the respective quadrics : theorem 1 gives the result.
The map **c** defining the code ( see § 1 ) is one to one, and thus the dimension of the code is equal to the dimension of $\mathbf{F}_q[X_0,\ldots,X_n]_1^0$ over $\mathbf{F}_q$ , i.e. $n+1$ : indeed, if H is a hyperplane of $\mathbf{P}^n(\mathbf{F}_q)$, ( which amounts to taking a linear form of $\mathbf{F}_q[X_0,\ldots,X_n]$ ), it is sufficient to apply the results of Theorem 2 to see that $|Q \cap H| < |Q|$ , and to have also the different weights. ♦

## 4. Projective Reed-Muller codes of order 2 associated to a quadric

The map $\mathbf{c} : \mathbf{F}_q[X_0,\ldots,X_n]_2^0 \to \mathbf{F}_q^{|Q|}$ as introduced in § 1 defining the projective Reed-Muller code of order 2 associated to the quadric Q has for domain the vector space of quadratic forms over $\mathbf{F}_q$ ; this is why we gave previously some results on the intersection of two quadrics of $\mathbf{P}^n(\mathbf{F}_q)$.

**Theorem 7** (parabolic case) : Let Q be a parabolic quadric in $\mathbf{P}^n(\mathbf{F}_q)$, $n \geq 2$. If $q \geq 8$ then the projective Reed-Muller code of order 2 associated to Q has the following parameters :

$$\text{length} = \pi_{n-1},\ \text{dimension} = \frac{n(n+3)}{2},\ \text{distance} \geq q^{n-1} - 6\,q^{n-2} - \frac{q^{n-1}}{q-1}\,.$$

**Theorem 8** (elliptic case) : Let Q be an elliptic quadric in $\mathbf{P}^n(\mathbf{F}_q)$ of rank $r > 2$. If $q \geq 8$ then the projective Reed-Muller code of order 2 associated to Q has the following parameters :

$$\text{length} = \pi_{n-1} - q^{(2n-r)/2},\ \text{dimension} = \frac{n(n+3)}{2}\,,$$

$$\text{distance} \geq q^{n-1} - q^{(2n-r)/2} - 6\,q^{n-2} - \frac{q^{n-1}}{q-1}\,.$$

We reserve the case where the quadric is hyperbolic of rank 2 for the theorem 10 (we have indeed more precise results).

**Theorem 9** (hyperbolic case of rank $r \geq 4$) : Let Q be an hyperbolic quadric in $\mathbf{P}^n(\mathbf{F}_q)$ of rank $r \geq 4$. If $q \geq 8$ then the projective Reed-Muller code of order 2 associated to Q has the following parameters :

$$\text{length} = \pi_{n-1} + q^{(2n-r)/2}, \text{ dimension} = \frac{n(n+3)}{2},$$

$$\text{distance} \geq q^{n-1} + q^{(2n-r)/2} - 6\,q^{n-2} + \frac{q^{n-1}}{q-1}.$$

Let us remark that we can have, for the theorem 9, the same results with a weaker hypothesis on q when the rank of Q is equal to 4 or 6, namely $q > 5$.

Now we consider the case of *maximal* quadrics, that is hyperbolic quadrics of rank 2. By the corollary of theorem 1, the number of points of these quadrics reaches the maximum number of points of a quadric, and it is in this sense that we call them "maximal". We can remark that they are particular quadrics (they are the union of two distinct hyperplanes). The codes which are associated to them have a minimum distance precisely known. These codes will have a generalization in the next paragraph.

**Theorem 10** (hyperbolic case of rank = 2) : Let Q be an hyperbolic quadric in $\mathbf{P}^n(\mathbf{F}_q)$ of rank 2. The projective Reed-Muller code of order 2 associated to Q has the following parameters :

$$\text{length} = \pi_{n-1} + q^{n-1}, \text{ dimension} = \frac{n(n+3)}{2}, \text{ distance} = q^{n-2}(q-1).$$

*Proof* : The length of the codes is the number of points of the quadric Q, and is given by Theorem 1.

Let $F' \in \mathbf{F}_q[X_0,\ldots,X_n]_2^0$ and $Q' = Z_{\mathbf{P}^n}(F')$, $Q = Z_{\mathbf{P}^n}(F)$.

Either F and F' are proportional, and then Q = Q'. Remark that there is $q - 1$ such non zero forms F' ; thus there is at least q quadratic forms vanishing in Q, hence in the kernel of the map **c** defining these codes. We claim that there are no other forms in Ker(c), and thus the dimension of this codes is :

$$\dim(\text{Im } c) = \dim \frac{\mathbf{F}_q[X_0,\ldots,X_n]_2^0}{\text{Ker}(c)} = \frac{(n+1)(n+2)}{2} - \log_q(|\text{Ker}(c)|)$$

$$\geq \frac{(n+1)(n+2)}{2} - 1 = \frac{n^2+3n}{2} = \frac{n(n+3)}{2}.$$

Indeed, suppose now that F and F' are not proportional, we have by Theorem 3 :

$$|Q \cap Q'| \leq \pi_{n-2} + \frac{7\,q^{n-1}}{q-1} - \frac{6\,q^{n-2}}{q-1}.$$

- if Q is parabolic (Th 7), we have

$$\pi_{n-2} + \frac{7\,q^{n-1}}{q-1} - \frac{6\,q^{n-2}}{q-1} < |Q| \Leftrightarrow q^2 - 8q + 6 > 0 \Leftrightarrow q \geq 8.$$

Moreover, F and F' cannot have a common factor of degree 1 since Q would be the union of two hyperplanes and thus would be hyperbolic.
The minimum distance follows from the same inequality of the Theorem 3.
- if Q is elliptic (Th 8), F and F' cannot also have a common factor of degree 1, and we have :

$\pi_{n-2} + \frac{7\,q^{n-1}}{q-1} - \frac{6\,q^{n-2}}{q-1} < |Q| = \pi_{n-1} - q^{(2n-r)/2}$ if and only if $q > 8$ for $r = 4$, and thus a fortiori for $r \geq 4$, i.e. since r is even, $r > 2$.
- if Q is hyperbolic of rank $\geq 4$ (Th 9), the same reasoning gives a fortiori the results (indeed the hypothesis $q \geq 8$ holds for more "smallest " quadrics).
- if Q is hyperbolic of rank = 2 (Th 10) :
* either F and F' have a common factor of degree 1, and by the Theorem 3 :

$$|Q \cap Q'| = \pi_{n-1} + q^{n-2} \text{ which is } < |Q| = \pi_{n-1} + q^{n-1}.$$

* or F and F' have not a common factor of degree 1, and by the lemma preceding Theorem 3 we have : $|Q \cap Q'| \leq \pi_{n-1} + q^{n-2}$ which is $< |Q|$.
The minimum distance in this case is :

$$|Q| - (\pi_{n-1} + q^{n-2}) = q^{n-1} - q^{n-2} = q^{n-2}(q-1). \blacklozenge$$

## 5. Projective Reed-Muller codes associated to a maximal hypersurface

We consider here hypersurfaces of degree $h \leq q$ reaching the Serre bound, i.e. which are the union of h distinct hyperplanes containing a linear variety of codimension 2. The Serre bound enunciated in § 2.1 has the following projective version : if F is a non zero form of degree $h \leq q$ of $\mathbf{F}_q[X_0,\ldots,X_n]$, then

$$|Z_{\mathbf{Pn}}(F)| \leq \pi_{n-2} + h\,q^{n-1}.$$

The construction of such varieties (called maximal) is easy ; indeed we can take for example :

$$F = \prod_{1 \leq i \leq h} (X_0 - \lambda_i X_1)$$

where the $\lambda_i$ are h distinct elements of $\mathbf{F}_q$. We are going to construct projective Reed-Muller codes associated to such varieties.

**Theorem 11** : Let $V = Z_{\mathbf{Pn}}(F)$ be a variety of $\mathbf{P}^n(\mathbf{F}_q)$ which is the union of h distinct hyperplanes containing a linear variety of codimension 2, with $h \leq q$. Then the projective Reed-Muller code of order $d < h$ associated to V has the following parameters :

$$\text{length} = \pi_{n-2} + h\,q^{n-1}, \text{ dimension} = \binom{n+d}{d}, \text{ distance} = (h-d)\,q^{n-1}.$$

Let us remark that we find again the projective Reed-Muller codes of order 1 associated to a maximal quadric (in the particular case $h = 2$ and $d = 1$).

*Proof* : The length of the code is equal to the number of points of the variety V which is, by construction,

$$\pi_{n-2} + h\, q^{n-1}.$$

The map $\mathbf{c}: \mathbf{F}_q[X_0,...,X_n]_d^0 \rightarrow \mathbf{F}_q^{|V|}$ defining the code is obviously one to one since $d < h$. Thus the dimension of the code is equal to the dimension, over $\mathbf{F}_q$, of $\mathbf{F}_q[X_0,...,X_n]_d^0$ i.e. $\binom{n+d}{d}$.

If $V = H_1 \cup ... \cup H_h$ then the subvariety V' of degree d of V defined by $V' = H_1 \cup ... \cup H_d$ where the d hyperplanes are taken among the h defining V, is such that :

$$|V'| = \pi_{n-2} + d\, q^{n-1}.$$

Thus the minimum distance of the code is equal to :

$$|V| - (\pi_{n-2} + d\, q^{n-1}) = h\, q^{n-1} - d\, q^{n-1} = (h-d)\, q^{n-1}.\blacklozenge$$

We can say more if we consider the particular case of the codes above of order 1. Indeed, it is easy to see that the hyperplane sections of such maximal varieties have three possible sizes, namely $\pi_{n-1}$, $\pi_{n-2}$ or $\pi_{n-3} + h\, q^{n-2}$. Thus, the projective Reed-Muller code of order 1 associated to V (with $h > 1$) is a code with three weights :

$$w_1 = (h-1)\, q^{n-1}\ ,\ w_2 = h\, q^{n-1}\ ,\ w_3 = h\, q^{n-1} + (1-h)\, q^{n-2}$$

and with the following parameters :

$$\text{length} = \pi_{n-2} + h\, q^{n-1}\ ,\ \text{dimension} = n+1\ ,\ \text{distance} = (h-1)\, q^{n-1}\ .$$

## References


[1] Chakravarti I.M., *Families of codes with few distinct weights from singular and non-singular hermitian varieties and quadrics in projective geometries and Hadamard difference sets and designs associated with two-weights codes*, Coding Theory and Design Theory - Part I : Coding Theory IMA vol. **20**.

[2] Delsarte P., Goethals J.M. and Mac Williams F.J., *On generalized Reed-Muller codes and their relatives*, Inform. and Control **16** (1970) 403-442.

[3] Games R.A. , *The Geometry of Quadrics and Correlations of sequences*, IEEE Transactions on Information Theory. Vol. IT-**32**, No. 3, May 1986, 423-426.

[4] Hirschfeld J.W.P., *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[5] Kasami T., Lin S. and Peterson W.W., *New generalization of the Reed-Muller codes - Part I : Primitive codes*, IEEE Trans. Information Theory **IT-14** (1968), 189-199.

[6] Lachaud G., *The parameters of projective Reed-Muller codes*, Discrete Mathematics **81** (1990), 217-221.

[7] Manin Yu.I. and Vladut S.G., *Linear codes and modular curves*, Itogi Nauki i Tekhniki **25** (1984) 209-257 J. Soviet Math. **30** (1985) 2611-2643.

[8] Primrose E.J.F., *Quadrics in finite geometries*, Proc. Camb. Phil. Soc., **47** (1951), 299-304.

[9] Ray-Chaudhuri D.K., *Some results on quadrics in finite projective geometry based on Galois fields*, Can. J. Math., vol. **14**, (1962), 129-138.

[10] Schmidt W.M., *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Maths **536** (1975).

[11] Serre, J.-P., *Lettre à M. Tsfasman, 24 juillet 1989*, Journées Arithmétiques de Luminy, Astérisque, S.M.F., Paris, to appear.

[12] Sorensen A.B., *Projective Reed-Muller codes*, to appear.

[13] Wolfmann J., *Codes projectifs à deux ou trois poids associés aux hyperquadriques d'une géométrie finie*, Discrete Mathematics **13** (1975) 185-211, North-Holland.